

IDENTITY, TRUST AND SECURITY

Identity in the Age of AI and Quantum Computing

Why proving who and what we can trust is becoming a foundational security problem.

EXECUTIVE SUMMARY

Artificial intelligence is making convincing impersonation, synthetic media and personalised social engineering cheaper and more scalable. At the same time, future cryptographically relevant quantum computers threaten public-key algorithms that underpin digital signatures, certificates and identity systems. The shared issue is trust: **AI makes identity easier to imitate, while quantum computing threatens parts of the cryptographic layer used to prove authenticity.**

PERSON

IDENTITY

CRYPTOGRAPHY

TRUST

AI Changes the Economics of Impersonation

Identity fraud is not new. What AI changes is the cost, speed and quality of creating convincing evidence around a false identity.

A public profile photograph may provide material for facial comparison, correlation across platforms or synthetic media. Voice samples can contribute to voice cloning. Public employment histories and social activity can be assembled into highly personalised narratives. Generative AI can produce polished communications without many of the mistakes that once exposed phishing attempts.

The question is no longer only, “Does this person know the correct password?” It is, “What evidence do we have that the person, device, credential and transaction are genuine?”

A photograph alone should not defeat a well-designed biometric system. Modern proofing can incorporate live capture, presentation-attack detection, sensor integrity and device controls. But NIST now explicitly addresses

Identity Becomes the Security Perimeter

Traditional organisational boundaries are fading. Employees work remotely, customers use unmanaged devices, contractors cross tenant boundaries, APIs communicate autonomously, and AI agents are beginning to act on behalf of humans and organisations.

That creates a broader assurance problem. Organisations need to distinguish between a legitimate human, a compromised account, an authorised workload, an approved AI agent and software merely claiming to act for somebody else.

THE PRACTICAL SHIFT

Authentication is necessary but no longer sufficient. Identity architecture must also establish who was enrolled, what authority they hold, which device or workload is acting, whether the credential remains valid, and whether the requested action was genuinely authorised.

What becomes more valuable

Passkeys

Device trust

Verifiable credentials

Workload identity

Provenance

Then Comes the Quantum Problem

Much of today's digital trust depends on public-key cryptography. Certificates, secure communications, software signing, identity assertions and many credential systems rely on algorithms such as RSA and elliptic-curve cryptography.

A sufficiently capable cryptographically relevant quantum computer using algorithms such as Shor's algorithm could undermine these widely deployed schemes. Symmetric cryptography and hashing are affected differently, but public-key cryptography is deeply embedded throughout modern infrastructure.

This matters for identity because a digital credential is trustworthy only if a verifier can determine that an authorised issuer signed it and that the content has not been altered. If the signature algorithm becomes unsafe, the issue is not merely confidentiality. It becomes **a problem of authenticity**.

Two Risks, One Trust Problem

AI challenges whether the evidence we see and hear is genuine.

Quantum computing threatens some of the cryptography we use to prove what is genuine.

Between them sits identity.

What Organisations Should Start Doing Now

- Treat identity as a core security control, not merely an application login function.
- Reduce password dependence and adopt phishing-resistant authentication.
- Strengthen identity proofing against synthetic media, replay and injection attacks.
- Protect biometric data as highly sensitive and effectively non-replaceable.
- Bind high-risk transactions to explicit authentication and authorisation.
- Establish clear identities for humans, workloads, machines and AI agents.
- Replace unnecessary document copies with authoritative digital verification where appropriate.
- Inventory use of RSA, ECC and other cryptographic algorithms across certificates, APIs, applications and infrastructure.
- Design for **cryptographic agility** so algorithms and keys can be replaced without redesigning entire platforms.
- Build a post-quantum migration roadmap and test PQC or hybrid approaches where standards and products support them.
- Assess long-lived credentials, archives, signatures and confidential data for future migration or re-signing needs.
- Consider "harvest now, decrypt later" exposure where information must remain confidential for many years.

Conclusion: Trust Becomes Infrastructure

The AI and quantum transitions initially appear to be separate technology problems. They are not.

AI challenges our confidence in what we see and hear. Quantum computing challenges some of the cryptographic mechanisms

SELECTED REFERENCES

1. NIST, *Digital Identity Guidelines: Identity Proofing and Enrollment*, SP 800-63A-4.
2. NIST, *FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*, 2024.
3. NIST, *FIPS 204 - Module-Lattice-Based Digital Signature Standard (ML-DSA)*, 2024.