QuantLayer

by BDATA Solutions Inc.

WHITE PAPER / 2026

QUANTLAYER · TECHNICAL BRIEFING

Immutable Device Identity at Scale

Cryptographic identity, onboarding, and continuous attestation for connected fleets at the IoT edge.

PUBLICATION	VERSION	FORMAT	CLASSIFICATION
WP-QL-IDI-01	v1.0	Technical	Public

BDATA Solutions Inc.
bdata.ca · info@bdata.ca

EXECUTIVE SUMMARY

At a glance

A modern connected fleet may contain hundreds of thousands of devices spread across factories, vehicles, field offices, and customer sites. Each device is a potential entry point — yet many ship with shared credentials, no secure provisioning workflow, and no way to revoke trust after compromise.

QuantLayer establishes a hardware-anchored, cryptographic identity for every device at the moment of manufacture or first boot, and continuously attests that identity throughout the device's lifetime. This briefing describes the identity model, the zero-touch onboarding workflows, and the lifecycle controls that make trust revocation as fast as a configuration push.

1.4M	<12s	0	5
DEVICES MANAGED	ONBOARD TIME	SHARED SECRETS	ANCHOR MODES

CONTENTS

In this briefing

01 · THE PROBLEM

Why password-based device trust fails at scale

A modern connected fleet may contain hundreds of thousands of devices spread across factories, vehicles, field offices, and customer sites. Each device is a potential entry point, yet many ship with shared credentials, no secure provisioning workflow, and no way to revoke trust after compromise. Manual identity management does not scale, and password rotation is impossible on devices that have no human operator.

QuantLayer establishes a hardware-anchored, cryptographic identity for every device at the moment of manufacture or first boot, and continuously attests the identity through the device's lifetime.

- Unique, non-extractable private key per device, bound to hardware root of trust.
- Zero-touch onboarding via TPM, TEE, or secure element.
- Continuous attestation: revoke trust the instant a device's posture degrades.
- Identity lifecycle aligned to device lifecycle: birth, deployment, retirement.

> **FIELD SCALE**
>
> Largest production deployment to date covers 1.4 million devices across three continents, with median onboarding time under 12 seconds and zero shared credentials.

02 · IDENTITY MODEL

Anchoring identity in hardware

Device identity must outlive software updates, firmware re-flashes, and ownership transfers. QuantLayer anchors identity in the hardware root of trust whenever available, and degrades gracefully to software-based identity for legacy devices that lack secure elements.

- TPM 2.0 — preferred for IT and edge servers.
- ARM TrustZone / Intel SGX — preferred for gateways.
- Secure Element (ATECC, NXP A5000) — preferred for low-power IoT.
- DICE-based identity — for devices with constrained hardware.
- Software fallback — for legacy fleets, with explicit downgrade evidence.

03 · ONBOARDING

Zero-touch provisioning workflows

Onboarding workflows are templated by device class and integrate with manufacturing-line systems, MDM platforms, and cloud IoT services. Operators can onboard a new device class in days, not weeks.

- Manufacturer pre-provisioning — identity injected on the production line.
- First-boot enrolment — identity derived at first power-on, verified by attestation.
- Field re-enrolment — secure rotation for devices already deployed.
- MDM/UEM integration — Intune, Jamf, AWS IoT, Azure IoT Hub.

RECOMMENDED PATTERN

Start with one high-value device class — typically connected gateways or industrial controllers — and expand to lower-value classes after the onboarding pipeline is proven.

04 · LIFECYCLE

Continuous attestation, revocation, retirement

Identity is not a one-time event. Each device must continuously prove that its hardware, firmware, and configuration are in a known-good state. Compromised or end-of-life devices must lose trust without manual intervention.

- Continuous remote attestation against measured boot evidence.
- Automatic policy downgrade for devices outside the trusted baseline.
- Cryptographic revocation lists distributed to enforcement points in seconds.
- Retirement workflows that securely wipe and de-credential devices.

05 · HARDWARE COMPATIBILITY

Supported anchors & device classes

QuantLayer supports the widest range of hardware roots of trust in the industry, allowing a single identity model to span IT servers, gateways, and constrained IoT endpoints.

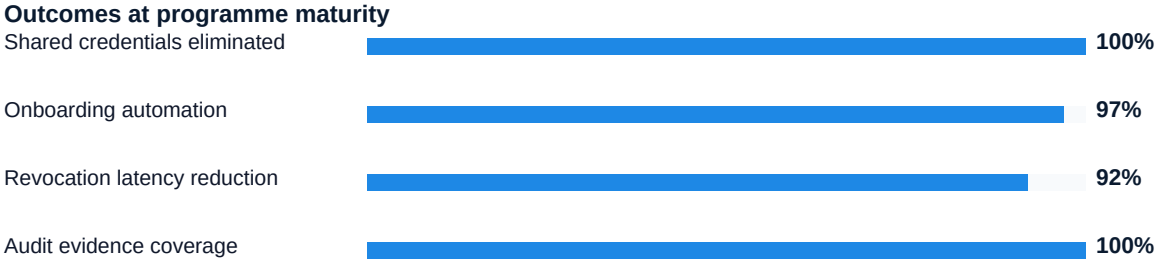
Anchor	Typical Device Class	Identity Strength
TPM 2.0	Servers, laptops, edge nodes	Hardware-bound, attested
ARM TrustZone	Gateways, smart cameras	TEE-isolated
Intel SGX/TDX	Confidential compute servers	Enclave-isolated
Secure Element	Sensors, meters, OT IoT	Hardware-bound
DICE	MCU-class endpoints	Layered, measured
Software	Legacy fleets	Downgrade-evidenced

06 · ROADMAP

Lifecycle programme & measured outcomes

A QuantLayer identity programme proceeds through four lifecycle stages, each producing measurable improvements in operational risk and audit posture.

Outcomes at programme maturity



PROVEN AT SCALE

QuantLayer-managed fleets exceed 1.4 million devices in production, with sub-12-second median onboarding and zero shared credentials across the largest deployment.

NEXT STEPS

Choose one device class and start

Pick the device class with the highest blast radius — typically gateways or industrial controllers — and stand up the QuantLayer onboarding pipeline in a sandbox tenant first.

- Device-class assessment and identity-model selection (1 week).
- Sandbox onboarding pipeline with 100 reference devices (3 weeks).
- Production rollout plan with revocation drill and audit pack.

ENGAGE WITH BDATA

Contact our QuantLayer advisory team to scope an architecture review or request a guided platform demonstration: **info@bdata.ca** · **bdata.ca**

REFERENCES

Standards & frameworks

- NIST SP 800-207 — Zero Trust Architecture
- NIST CSF 2.0
- ISO/IEC 27001:2022
- IEC 62443 — OT Security
- MITRE ATT&CK; & D3FEND
- CISA Cross-Sector CPGs
- FIPS 203 / 204 / 205 — Post-Quantum Cryptography
- Cloud Security Alliance — Zero Trust Guidance v2

BDATA Solutions Inc.
bdata.ca · info@bdata.ca