AegisEdge®

Identity at the Edge

Technical Overview

AegisEdge® GmbH, Frankfurt (Hessen), Germany

Security at the edge. Before the cloud.

Website: https://aegisedge.net

Email: info@aegisedge.net

Version 1.3, February 2026

Abstract

The **AegisEdge Node** is a hardened edge device that anchors identity and cryptographic operations in a **Hardware Root of Trust** and manages keys and updates through a **Post-Quantum Cryptography (PQC)**-resistant lifecycle. This technical overview summarizes what the Node does and how it fits into the AegisEdge system: identity and key management at the edge, revocable credentials, PQC-signed over-the-air updates, and local multimodal biometric verification, with sensitive keys and data kept on-device.

Figure 1: AegisEdge Node.

1 What We Do

In high-assurance environments, such as critical infrastructure, defense, automotive, and enterprise, the identity and cryptographic key management must be tamper-resistant, future-proof, and revocable. The AegisEdge Node is the on-device component of an architecture that provides the following:

- **Hardware Root of Trust** security: identity and key material are bound to a secure enclave with unclonable device binding.
- **PQC-resistant** design: identity and operational keys use NIST-standardized post-quantum algorithms.
- **Revocable keys**: certificates and operational keys can be revoked when needed via a central authority.

The Node performs local biometric verification, holds private keys in hardware, and participates in a defined PQC Key Management and Identity Lifecycle with the AegisEdge Provisioning Service. It is the secure, PQC-aware device that owns its identity and runs local biometric and security logic while interacting with the Provisioning Service only for certificate issuance, operational key distribution, and signed updates.

2 The AegisEdge Node at a Glance

The Node is a physical edge appliance or module that:

1. **Hosts a Hardware Root of Trust** that generates and stores the device's long-lived identity key pair and never exports the private part.
2. **Stores and uses cryptographic keys** for identity and for secure operations (device-to-device or device-to-service communication), all inside a secure enclave.

(a) Portable AegisEdge Node.

(b) AegisEdge Wearable.

Figure 2: AegisEdge Node form factors.

3. **Performs local multi-modal biometric verification** (e.g., fingerprint, face, cardiac rhythm) and AI-based liveness and matching. Biometric templates and verification stay on-device; no raw biometric data is sent to the cloud.
4. **Participates in provisioning and updates**: it registers with the AegisEdge Provisioning Service, receives a PQC-signed identity certificate and an operational key pair, and accepts only PQC-signed over-the-air updates that are verified before installation.

After provisioning, the Node uses its credentials to authenticate to other Nodes or backend services and to protect those channels.

3 How It Works

The Node operates as one of three main elements: the **Hardware Root of Trust** (on-device), the **AegisEdge Node** (the device), and the **AegisEdge Provisioning Service** (backend, acting as Certificate Authority). The Root of Trust generates a device-unique identity key pair and keeps the private key inside the enclave. The Node registers with the Provisioning Service, proves possession of that identity, and receives a PQC-signed identity certificate and an operational key pair. Once provisioned, the Node can perform local biometric verification, authenticate to peers and services, and receive only PQC-signed over-the-air updates that are verified against the Root of Trust before installation.

Revocation. When a key or device must be decommissioned (e.g., compromise, loss, or end-of-life), the Provisioning Service revokes the corresponding credentials and maintains a signed revocation list. That list is distributed to all entities that verify credentials, so revoked certificates and keys are no longer accepted. Revocation is initiated only by authorized administrators; it can be permanent (the Node is excluded from the system) or temporary (the Node can be re-provisioned with new credentials). The system thus supports revocable keys end-to-end without exposing internal procedures.

4 Key Features

- **Hardware Root of Trust with unclonable device binding** for identity key generation and storage.

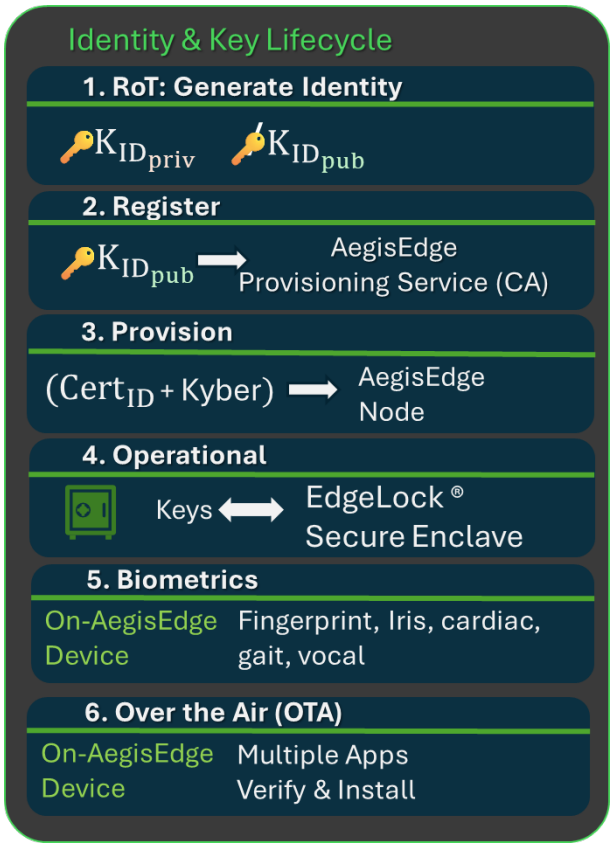

Figure 3: Identity & key lifecycle: from key generation to operational use and updates.

- **PQC-resistant** identity and operational keys (NIST-standardized algorithms).
- **Revocable keys** via the Certificate Authority and a maintained revocation list.
- **Multi-modal biometrics and AI** on-device; biometric data stays inside the device.
- **Secure key storage** in the secure enclave.
- **PQC-signed over-the-air updates** verified against the Root of Trust before installation.

Together, the Root of Trust, the Node, and the Provisioning Service form a **PQC-resistant**, **hardware-anchored**, **revocable** identity and key management system for high-assurance deployments at the edge.

AegisEdge System Summary

The **AegisEdge Node** anchors identity in a Hardware Root of Trust, performs local multi-modal biometric verification, and participates in a PQC Key Management and Identity Lifecycle with the AegisEdge Provisioning Service. The Node obtains and stores identity and operational keys, supports revocable keys and PQC-signed OTA updates, and keeps sensitive keys and data inside the device. Together, the RoT, the Node, and the Provisioning Service form a **PQC-resistant**, **hardware-anchored**, **revocable** identity and key management system suitable for high-assurance deployments at the edge.