

Roost is a 2U rack signing appliance. Three voting chips from three different manufacturers sign as a 2-of-3 quorum, a separate monitor watches every request, and each key is regenerated from the silicon itself at power-up. No key is stored.

Built to the requirements of FIPS 140-3 and KCMVP, Roost is protected in layers: an outer steel shell with tamper seals, security screws and a lid switch; an inner enclosure sealed with a detection mesh on all six faces; and instant erasure on detection, together with temperature and voltage defenses.

PHYSICAL

Form factor	2U, 19-inch rack mount
Dimensions (W × D × H)	436 × 400 × 88 mm
Cooling	Front-to-back airflow
Power	100–240 V AC, IEC C14 inlet
Network uplink	1 × RJ45 Ethernet

SIGNING ARCHITECTURE

Voters	3 signing chips, each from a different manufacturer
Monitor	1 separate device that does not sign: records every request, detects anomalies, blocks requests
Controller	1 controller for networking and request handling
Quorum	2-of-3: signing continues if one voter fails; a single compromised voter cannot sign
Key handling	PUF keyless: each voter regenerates its key from its own silicon at power-up; keys are never stored, exported or backed up

PHYSICAL SECURITY

Enclosure	Sealed tamper-sensing inner enclosure with detection mesh on all six faces; power supply outside the mesh
Tamper response	Opening, cutting or drilling erases the values needed to regenerate each PUF key, so it can never be produced again; erasure works even with power off, and signing stops
Tamper monitoring	Separate battery-backed monitor board inside the mesh: lid and base switches, cable entries and light; fails secure (ends erased) if the battery runs out; tamper-evident chain record of every detection
Environmental protection	Per-chip temperature sensors, per-rail voltage monitoring, voltage-glitch and clock-anomaly detection; out-of-range conditions are treated as an attack
Deployment	Closed network, on-premises; no outbound connection required

STANDARDS

Requirements	Complies with the requirements of FIPS 140-3, KCMVP and the EU Cyber Resilience Act (Regulation (EU) 2024/2847)
--------------	---