PARTNER CONTENT

Vincent Korstanje

CEO

Kigen

SECURING THE INTELLIGENCE ERA: PHYSICAL AI DEMANDS UPDATEABLE TRUST

MWC BARCELONA 2026 IS CALLING THIS MOMENT THE IQ ERA. WE ARE ENTERING AN ERA IN WHICH AI NO LONGER LIVES SOLELY IN THE CLOUD, BUT IN AUTONOMOUS MACHINES, SENSORS AND ROBOTICS THAT INTERACT WITH THE PHYSICAL WORLD.

As AI models shrink and chips become more capable, resident AI on small endpoints may become the norm in the coming years. This shift is increasingly described as Physical AI: systems that perceive, reason and act in the physical world.

As on-device AI models become more capable, intelligence can be device-native, distributed and diverse. To users, these endpoints can feel like sentient AI because they respond, adapt and act in real time. This new era demands a new paradigm in security: **Physical AI must be trusted to be useful and stay secure**.

Trust starts with secure device identity. At scale, every security decision begins by questioning what each device is in reality.

Kigen

The mobile ecosystem offers a proven foundation. The eUICC, more commonly known as the eSIM, provides tamper-resistant storage for credentials. This identity, when combined with essential utilities, makes the eSIM a durable anchor for onboarding, authentication and security updates for the product across long device lifetimes.

Physical AI endpoints are long-lived and adversaries are adaptive. Trust must be renewable, because vulnerabilities will be discovered after deployment. Regulation is now making this explicit. The EU Cyber Resilience Act entered into force in December 2024; reporting obligations apply from September 2026 and the main obligations from December 2027.

Those dates overlap with design decisions being made now for devices that must remain patchable and supportable for years.

The GSMA's IoT eSIM RSP standard, widely known through SGP.32, was designed for constrained devices and introduced the eSIM IoT Remote Manager (eIM) for scenarios with limited connectivity and no user interface. It is remote SIM provisioning (RSP) optimised for the realities of IoT. Read through a security lens, it does two decisive things for Physical AI. It anchors cryptographic material, such as identity, subscription credentials and sensitive lifecycle keys, in a secure element. And it provides an operational control plane for remotely managing connectivity states, with auditable intent and policy enforcement.

Trustworthy AI outcomes depend on secure boot and secure communications, but also on the ability to patch, rotate credentials and recover when assumptions break. Updates can no longer be treated as an afterthought. They are the inf rastructure that keeps Physical AI trustworthy over time. The most successful Physical AI experiences will not be the most autonomous in a demo, but the most dependable years later after vulnerabilities are discovered, fixes are issued and fleets are patched without disruption. In practice, manufacturers investing in eSIM-first Physical AI devices are increasingly prioritising one capability above all others: **the ability to update the eSIM OS itself if an issue ever arises**.

This is the real inflection point: the emergence of an eSIM operating system that spans SIM, eSIM and iSIM, works across different RSP architectures and can dynamically detect and seek security updates, paired with a fully SAS-certified, robustly tested and hosted eIM capable of operating at fleet scale. Together, they enable something the industry has struggled with for years: the ability to patch Physical AI device fleets reliably, securely and at scale.

As MWC Barcelona 2026 sharpens the conversation around this new IQ era, I'd recommend four developments worth exploring:

First, **MFF4 form factors**, enabling secure identity in as little as 2×2mm². Physical AI is moving into ever-smaller devices, where every millimetre counts. MFF4-class eSIMs make it possible to embed secure device identity even in the most compact nodes, already familiar territory for eSIM-first smartwatches, and prompt an important question: how compact can AI endpoints get and still serve moments that we marvel at?

Second, an **eSIM OS with dynamic patching**. A compact, IoT-tuned eSIM OS becomes a root of trust across diverse devices. What matters most is choosing an OS designed for the intelligence era, one that can actively participate in security update workflows, bringing the best of user-elected or manufacturer-pushed critical fixes.

Third, **an eIM built for scale and real-world conditions**. Physical AI fleets do not update like smartphones. Connectivity is intermittent, devices may not be directly accessing the public internet, downloads may be interrupted and campaigns must tolerate queuing and retries. A fully SAS-certified eIM built for SGP.32, with functionality that addresses these realities, makes secure operations repeatable, auditable and resilient, turning remote updates from risk into routine.

Finally, **an ecosystem committed to security**. Physical AI rarely starts from a clean slate. Some organisations migrate legacy SIM estates, others retrofit deployed fleets and others scale digital distribution at internet speed. Interoperability, testing and certified pathways matter for the operational reality of scaled deployments.

Some companies are already helping others to migrate: **NuvoLinQ** has described "leaving no legacy SIM behind" for point-of-sale and automated transactions. Others want to retrofit fleets across product portfolios, as industrial router makers such as **Robustel** do. And others want to scale digital distribution, such as travel eSIM services that see demand of around 100,000 eSIM downloads per day. Different starting points, same requirement: identity you can trust and change you can control.

MWC Barcelona 2026 will showcase Physical AI coming to life. Yet the real story is the quiet machinery behind it: with eSIMs evolving into an updateable root of trust, we gain a new licence to innovate, safely, at scale and for the long life of every device. May we build this intelligence era on trust that can be renewed, proven and shared so its benefits endure for everyone.

Kigen is a frontrunner in eSIM and iSIM technology, enabling hypergrowth telecom operators and device makers. Book a visit to experience the latest innovations in eSIM security at https://kigen.com/mwc-26/