Hardware-Enabled Governance Mechanisms

hardware-enabled-governance · compute · concept

Source: https://policywindow.org/wiki/hardware-enabled-governance

Generated 2026-11-19T01:06:00 UTC

Summary

Hardware-enabled governance mechanisms (HEGMs, also "on-chip governance" or hardware-enabled mechanisms/HEMs) propose to make AI-governance rules attach to the physical compute layer — AI accelerators (GPUs/ASICs), their firmware, and the datacenters that house them — rather than to actors' self-reports. The aim is to convert compute, an unusually concentrated and excludable input to frontier AI, into a verifiable governance chokepoint. Proposed mechanisms span four families: (1) cryptographic attestation and compute-usage logging that lets a chip prove what workload it ran (e.g., training-run accounting to verify a compute-threshold rule); (2) location verification, typically delay-based geolocation in which a trusted "landmark" server measures a chip's signed-challenge response time to bound its physical location and detect diversion; (3) on-chip usage/licensing controls that can throttle, gate, or disable a chip absent an authorization (a "feature lock" or remote attestation requirement); and (4) tamper-evident/tamper-resistant packaging so the above cannot be silently bypassed. Across these, the load-bearing premise is a hardware root of trust — a per-chip private key that cannot be extracted by an adversary with physical access. The concept underpins both unilateral export-control enforcement (proving a chip is where it was licensed to be) and proposed multilateral, privacy-preserving compliance verification (e.g., flexible hardware-enabled guarantees, "flexHEGs"), where chips would attest compliance with an international agreement without exposing model weights, data, or hyperparameters.

At a glance

Used by

0 instrument(s)

Related concepts

compute-threshold, frontier-tier, ai-supply-chain, policy-instrument

Primary source

Aarne, O., Fist, T., & Withers, C. (2024). Secure, Governable Chips: Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing. Center for a New American Security (CNAS), January 8, 2024.

Details

Covers the physical-compute governance lever: on-chip attestation, compute monitoring/verification, location verification, usage/licensing locks, tamper resistance, and their use for export-control enforcement and proposed multilateral compliance verification. In scope: governance functions that bind to specific accelerators or datacenters and rely on a hardware root of trust. Out of scope: (a) compute-as-a-regulatory-threshold where the FLOP estimate is self-reported or architecture-derived rather than hardware-enforced (see compute-threshold); (b) administrative export controls that operate on paperwork/end-use licensing without any on-chip enforcement (see compute-export-controls); (c) software-only model-side governance (watermarking, evals, KYC at the API layer); and (d) datacenter physical security generally, except where it is the substrate for chip-level attestation. The boundary case — Nvidia's December 2025 software-based location verification using existing confidential-computing features —

sits at the edge of scope: it is a chip-assisted but not hardware-hardened mechanism and illustrates the gap between deployed software features and a tamper-resistant on-chip regime.

How to cite this article

APA

Policy Window. (n.d.). Hardware-Enabled Governance Mechanisms [Wiki article — Concept]. https://policywindow.org/wiki/hardware-enabled-governance

CHICAGO

Policy Window. n.d.. "Hardware-Enabled Governance Mechanisms." Wiki article (Concept). https://policywindow.org/wiki/hardware-enabled-governance.

HARVARD

Policy Window (n.d.) 'Hardware-Enabled Governance Mechanisms', Wiki article — Concept, available at: https://policywindow.org/wiki/hardware-enabled-governance.

OSCOLA

Policy Window, 'Hardware-Enabled Governance Mechanisms' (Wiki article — Concept, n.d.) <https://policywindow.org/wiki/hardware-enabled-governance> accessed [date].

BIBTEX

```
@misc{policywindow-hardware-enabled-governance,
title  = {Hardware-Enabled Governance Mechanisms},
author = {Policy Window},
year   = {n.d.},
howpublished = {hardware-enabled-governance — compute},
url    = {https://policywindow.org/wiki/hardware-enabled-governance},
note   = {Primary source: https://www.cnas.org/publications/reports/secure-governable-chips}
}
```