Behavior as First-Class Address in Intention Space

In Intention Space, behavior is elevated to a **first-class address** within the computational framework. This means that every meaningful act—such as registration, login, sending a message, or issuing a command—is not only executed but anchored through a **Common Path of Understanding and Execution (CPUX)**. Unlike traditional systems that rely on device-specific identifiers (e.g., MAC addresses, biometrics, or IP-based tokens), Intention Space ensures security and accountability through **behavioral consistency**. A CPUX encodes not just what was done, but also *why*, *by whom*, and *in what context*—verified by the alignment of gatekeeper PnRs and runtime trails. Spoofing a device or identity is insufficient; if a CPUX cannot be traced back to a legitimate and contextually aligned anchor (such as a prior registration or login CPUX), it is automatically invalidated. Thus, Intention Space enforces trust by checking whether a new action is a **natural continuation of prior intent**—not by the external identity alone, but by its position in the evolving behavioral trace.

Key Implications: Every CPUX carries its own provable behavioral trail. Device identifiers are optional—not required for verifying legitimacy. Gatekeeper PnRs enforce continuity across time and context. Behavior becomes the trusted fingerprint of a session. Consistency replaces static identity as the basis of authorization.