Abstract

An integrated credential-management platform (Fig. 1) automates the issuance, validation and life-cycle control of professional credentials. Activity data captured from electronic records and networked devices are transformed, in real time, into tamper-evident micro-credentials recorded on a permissioned distributed ledger. A machine-learning module continuously computes risk scores from credential histories and external outcome data to support predictive privileging decisions. High-stakes procedures are confirmed through dual biometric signatures that generate cryptographically verifiable supervision records. Clinical privileges are represented as smart-contract objects containing time, volume or training conditions that self-execute to grant, suspend or revoke access when parameters change. A natural-language regulatory scanner adds new credential requirements as rules evolve, while an API gateway blocks workforce-scheduling or system-access requests if corresponding privileges are invalid. Privacy-preserving sanction checks are performed with zero-knowledge non-membership proofs against revocation accumulators. The architecture thus provides a self-auditing, cross-institution credential and privilege framework.