Agentic AI Identity Management Needs a Hardware Root of Trust

Trusted agents: identity, protected model/config, attestation, and high-impact actions

Authors: Jorge Perez, Mario Lamberger

ITU-T Workshop 2026 | Session 4 | Geneva | 2 June 2026

Agentic AI has crossed the trust boundary.

1 **From advising to acting**

Agents now trigger purchases, approvals, payments, and enterprise workflows.

2 **The gap is identity + attestation**

Trust requires proof of which agent acted, on whose behalf, under what authority, and in what runtime state.

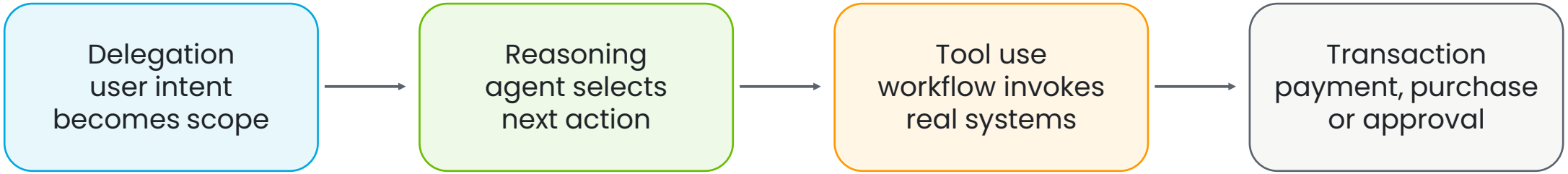
3 **Release credentials only after proof**

Critical actions may require confidential data; credentials should be released only to attested, uncompromised agents or runtimes.

Secure Elements can provide hardware-rooted custody for agent identity, delegated authorization, credential release, and policy-controlled approval.

The Problem Statement

Without identity-based trust and runtime proof, agentic AI does not scale safely and securely to high-impact use cases.



Example risk patterns

- **Confused deputy:** agent exceeds delegated authority
- **Runtime/memory poisoning:** short- or long-term memory alters behavior
- **Control-flow deviation:** reasoning drifts into unsafe tool use
- **Cascading trust failure:** compromised peer or tool propagates risk

Ecosystems still lack

- Verifiable agent identity
- Credential release conditioned on attestation
- Memory protection and runtime monitoring
- Continuous verification — not perimeter trust

Main Architectural Concepts

Make identity, protected model/config, and attestation first-class with a hardware root of trust underneath.

C1	Agent Identity & Authorization Agent name, user delegation, scope, purpose, duration, limits
C2	E2E Model & Agent Config Protection Signed model/config, protected policy store, load/update provenance
C3	Agent Attestation Evidence of agent, endpoint state, runtime, and model/config integrity
C4	Action & Transaction Assurance Bind intent, approval, execution, outcome; sign high-impact actions
HW RoT	Secure Element Hardware Root of Trust Non-exportable keys, user presence, tamper-resistant proof generation

Where Secure Elements Fit

Key message

Secure Elements add a device-level trust anchor for credentials, attestation, and high-impact actions — complementing cloud identity, protocols, and HSMs.

What this enables for the main components

- Device-bound identity & delegation keys
- Local custody of credentials and tokens
- Protected config hashes and policy data
- Attestation evidence for device, wallet, model/config, and runtime state
- Policy-gated signing and user presence for high-impact actions

NXP deployment context: payment, identity, mobile, automotive, and embedded security across edge devices. SEs raise resistance to advanced attackers through protected key storage, cryptographic operations, and attestation support..

Standards Relevance for ITU

ITU can define common vocabulary for agent identity, protected configuration, attestation evidence, credential-release conditions, and proof formats across ecosystems.

Candidate work items

- Agent identity & authorization: naming, delegation, scope, duration, purpose
- Attestation profile: endpoint, wallet, runtime, model/config, memory-integrity claims
- Credential-release policy: conditions, requester proof, verifier checks
- Proof/audit format: intent, approval, execution, outcome, evidence chain
- Runtime monitoring: control-flow signals, alarms, red-team evaluation profiles

Framework alignment

- **OWASP MAESTRO / Garak:** threat taxonomy and red-team evaluation
- **CAMEL-style supervisors:** runtime control-flow monitoring patterns
- **SPIFFE/SPIRE + A2A/MCP/ACP:** workload and agent-to-agent trust
- **PSA Certified / DICE / SPDM:** hardware attestation profiles

HW Root of Trust + attestation

Secure Elements provide hardware-backed keys, protected policy/config material, local credential custody, and attestation evidence for edge and embedded agents.

Proposal to ITU and ecosystem partners

Focus the first iteration on common vocabulary, credential-release policy, attestation evidence, verifier behavior, and hardware-rooted proof.

1

Define

Common vocabulary for agent identity, delegation, and credential-release conditions

2

Specify

Attestation claims, verifier behavior, and proof/audit formats

3

Pilot

High-impact actions with hardware-rooted credential custody

4

Validate

Red-team and evaluation profiles for runtime and memory protection

Get in Touch

Jorge Perez
NXP Semiconductors — CTO CCC&S

jorge.perez7@nxp.com

NXP Public | ITU-T Workshop 2026 | Session 4

nxp.com