TECHNICAL CONTRIBUTION / OWNER REVIEW

HTTP6

Technical Contribution: Human-Originated Agent Authority and Payload-Bound Messages

Frank Dylan Rosario; Lin Wang; Octavia Sulea; Francisco Perez; Dawn Lipscomb; Maxwell Calixto; Robert Bloodgood III

Dr. Taher Elgamal — Advisor and contributor

November 10, 2026

NIST NCCoE discussion package — not submitted

Requested action

We request technical feedback on the HTTP6 architecture and discussion of a bounded demonstration for the NCCoE agent-identity and authorization effort. The proposal concerns distinct workload instances, authenticated parent–child provenance, monotonically constrained permissions, and fresh proofs bound to complete application payloads. The Human Admission Client supplies the human-facing admission interface, while the Rosario–Wang construction supplies the private-reference membership component.

The supplied materials consist of the complete available architecture specification, mathematical formalizations, executable review profile, schemas, worked examples, and a reproducible validation kit. The packet identifies the implemented reference profile separately from the native-channel target. It asks for review and suitable project routing; it does not request a generic product certificate or represent an assigned HTTP version.

Contribution and institutional fit

An agent may act long after its user has completed a login and may create several descendant workers. The proposed architecture preserves a bounded origin of authority through that progression. The human authorizes a root scope, the root admits a distinct child under an authenticated policy, and the resource requires a fresh proof for the exact operation. Copying a previous record does not satisfy a new event's state, and a child's local permission change cannot replace the admitted ancestor ceiling.

The NCCoE agent-identity project currently accepts rolling feedback. Its announced first implementation use case is DevSecOps. The project's public summary emphasizes investigating existing standards together with extensions, enhancements, and profiles. We therefore propose a standards-compatible application demonstration while retaining the native HTTP6 channel as a separately specified research objective. [1–3]

The complete source architecture covers service discovery, human and machine admission, independent service identity, handshake transcript binding, encrypted directional records, application request and response semantics, browser/workspace deployment, WASIX capabilities,

policy inheritance, route lifecycle, agent fleets, revocation, and three-tier disaster recovery. Its native cryptographic suite and wire encoding retain explicit release decisions. The supplied local script executes the membership construction and message gate; it is not represented as the complete native browser or TLS replacement.

Proposed bounded demonstration

A developer approves a task with designated repositories, tools, destinations, lifetime, and release restrictions. A protected root admits a scheduler. The scheduler creates separate build and test workers, each with its own key and narrower policy. Workers read approved inputs and write designated artifacts through the resource gate. Publishing to production is a separately approved operation. Human authentication time is recorded separately from machine activity and delegation lifetime.

The delivered executable uses a reporting-worker fixture as its concrete test workload. Adapting it to DevSecOps is proposed work. The demo should compare successful authorized execution with attempted destination substitution, artifact export, copied-instance use, unauthorized minting, concurrent replay, parent revocation, and stale-state recovery. Results should include the actual resource effect, not only a frontend success or rejection message.

Mathematics and security properties

The native response is a private dictionary name of a public membership cell, masked by an independent private residue. Correct verification follows by reversing the mask and dictionary. Calibration and a separating schedule permit authorized reconstruction. Under fresh independent private masks and the specified credential-independent public controls, every supported credential induces the same released-view distribution. Sequential conditional freshness preserves that result for every supported finite observation count, including a trillion. These are source-defined mathematical implications rather than a trillion-exchange benchmark. [4–5]

The payload-bound review envelope adds an independent HMAC over the exact statement and native witness. It supplies computational context authentication. The one-use ledger claims the first eligible authenticated response before native checking. The inherited-policy gate then evaluates current authority before permitting a local effect. Credential privacy, payload authenticity, one-use state, and least privilege are separate parts of the evidence.

The exact mask profile consumes fresh private material. The delivered 24-character RW-40 record uses 150 private mask bits; one trillion such records require 18.75 TB of continuously packed mask material before other overhead. A computational derivation profile requires its own claim and analysis. The submitted source does not convert a fixed-size seed into unlimited independent entropy.

Available executable evidence

A new November 10, 2026 run of the unchanged reconstructed kit passed 81 unit tests, 16 explicit payload scenarios, and two public native vectors. The local flow accepted 18 native proofs for

one admission, one mint, eight requests and eight responses, with eight local effects. A temporary HTTP/1.1 localhost carrier transported three requests and the harness checked three corresponding response proofs locally. The exact finite audit and a 10,000-record primitive benchmark also completed. The environment and exclusions are retained in the raw records. [6]

The kit uses only Python's standard library. Its private setup is represented by protected-role objects in one process; hardware labels are modeled. Synthetic payloads remain readable in the review carrier. The next integration assignments are separately secured endpoints, authenticated private-material provisioning, the selected encrypted transport, real key custody and attestation, a trusted interaction path, distributed durable state, and resource-specific adapters. Reviewers can reproduce the evidence presently supplied and identify the required evidence for each stronger profile.

Review materials and reading order

Material	Purpose
Complete Specifications Review	Current profile separation, exact executable contract, full original architecture with diagrams, mathematical attachment, schema and test index
Updated hereditary-authority theory	Four equations, thirty worked examples, current author credits, and cited SSL history
Per-Message Proof evidence paper	Payload binding, information-theoretic premise, test evidence, resource cost and deployment gates
Expanded NIST review volume	Twelve main chapters and twelve appendices, schemas, reference code and classification/evidence catalogs
Runnable validation kit	Source, 81-test suite, sixteen payload fixtures, two native vectors, one-command reproduction, full READMEs
Mathematical source set	Exact definitions, proofs, worked constructions, observer model, entropy accounting, and Lean declaration registry

The NIST mapping is a proposed engineering crosswalk. Its twenty-family and 106-outcome example coverage is not a claim that all NIST clauses have been assessed. A selected boundary, authoritative requirement inventory, parameter values, provider assignments, and actual assessment establish deployment satisfaction. Likewise, an underlying cryptographic module's validation is distinct from review of the complete protocol. [7]

Questions for the project team

We seek guidance on the most useful bounded use case, expected interoperability with existing agent identity mechanisms, evidence formats, relevant comparison configurations, and the appropriate participation mechanism. We also request guidance on routing a focused review of the private-reference construction and its composition with application authorization. The accompanying native-profile decision register identifies the exact additional deliverables needed before an independently interoperable native-channel claim.

References

[1] NIST NCCoE, agent identity and authorization project page, rolling feedback. Checked November 10, 2026. https://www.nccoe.nist.gov/projects/software-and-si-agent-identity-and-authorization

[2] NIST, September 29, 2026 agent identity announcement, DevSecOps use case and project contact. https://content.govdelivery.com/accounts/USNIST/bulletins/42d04b7

[3] NIST NCCoE, *Summary of Comments on the Concept Paper*. https://pages.nist.gov/nccoe-ai-identity/summary-of-comments.html

[4] *Rosario–Wang: Consolidated Construction*, September 16, 2026, §§3–10; included source.

[5] *HTTP6: Executable Rosario–Wang Proof and Observer Demonstration*, November 9, 2026; included attachment.

[6] `06_evidence/regeneration_2026-11-10/validation_report.json` and corresponding logs; new reference-model execution.

[7] NIST CMVP FAQs, SG-6, protocol versus module validation. https://csrc.nist.gov/projects/cryptographic-module-validation-program/faqs