

Agent Communications *(private)*

Internet Protocol - AC(p)IP

draft-eckert-catalist-acip-framework
draft-liu-agent-metadata-sync-protocol
draft-dunbar-agent-attachment

Presenter: Toerless Eckert, tte@cs.fau.de (Futurewei)
Co-Proponents: Bing (Leo) Liu, liubing@huawei.com
Linda Dunbar, linda.dunbar@futurewei.com

v0.4 12/16/2026

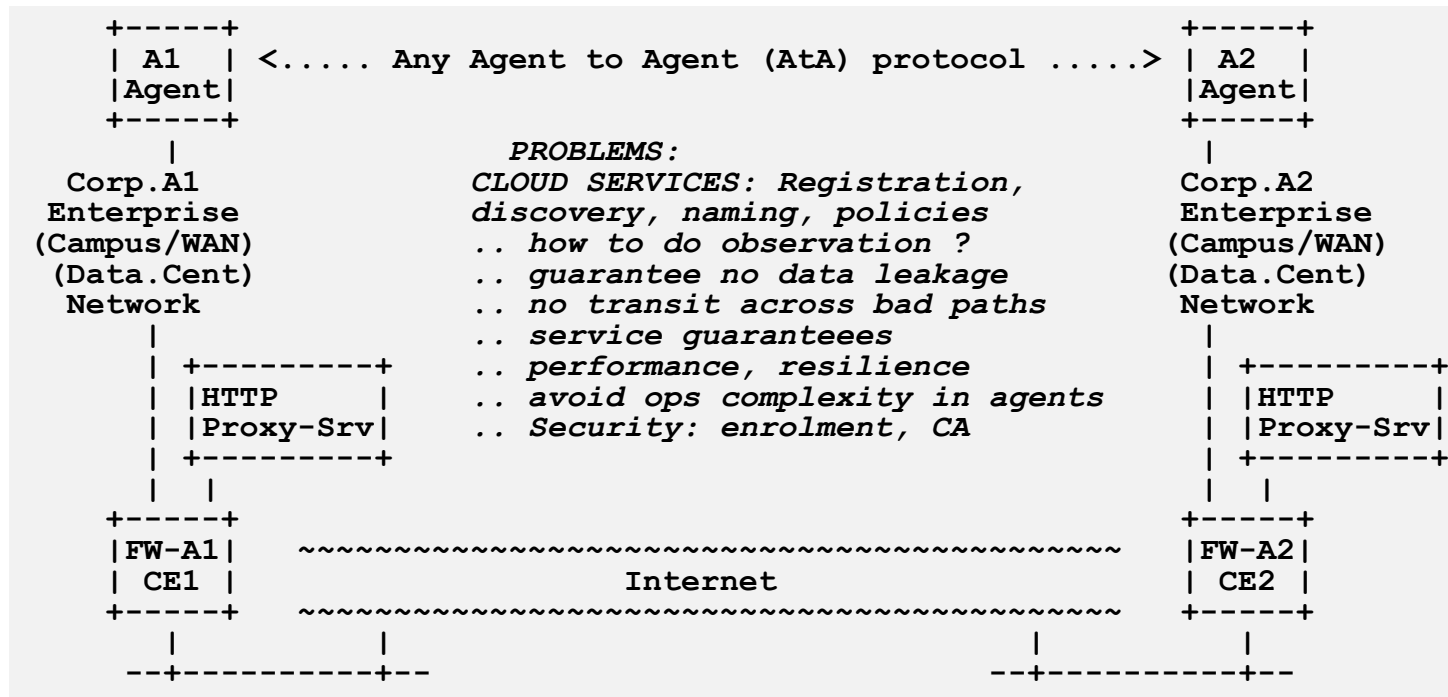
Managed secure private Internetworks for Inter Agent Communication Scenarios

- Reference use-case: ... Next-gen FinTech scenarios
 - HTTP B2B/B2C -> AI agent communications
 - Banks / Card Issuer, Payment Networks, Digital Wallet / Pay Interface, Merchants, App/User-interface, ATM ... operators – all with AI Agents
 - “Grown” network solutions: L2/L3/OTT/...Intra/Inter-provider private networks
 - + Various HTTP processing on “intermediate” nodes: forward proxy, “firewall”/WAF, reverse proxy, load-balancer, caches, CDN-edge, routing, DDoS protection, Security/Observability ...
 - Evolving private security network options, e.g.: SCION (mandatory for banking with Switzerland)
- Goal:
 - Develop new lightweight layer for intermediate nodes to **unify/simplify future AI agent scenario**
 - Evolution/simplification from hodgepodge of protocols using HTTP
 - Simple enough for consistent/easy manageable AND **processable by Tbps forwarding engines**
 - Keep HTTP end-to-end if Agent-to-Agent protocols use it
 - Past example: High Speed Trading (HFT) exceeded (CPU based) firewall performance
 - Dependency: Multi-layered security architecture:
 - Trusted middle-boxes, Trusted end-to-end (with trusted/regulated observability / security middle/men)

Reference Use-case

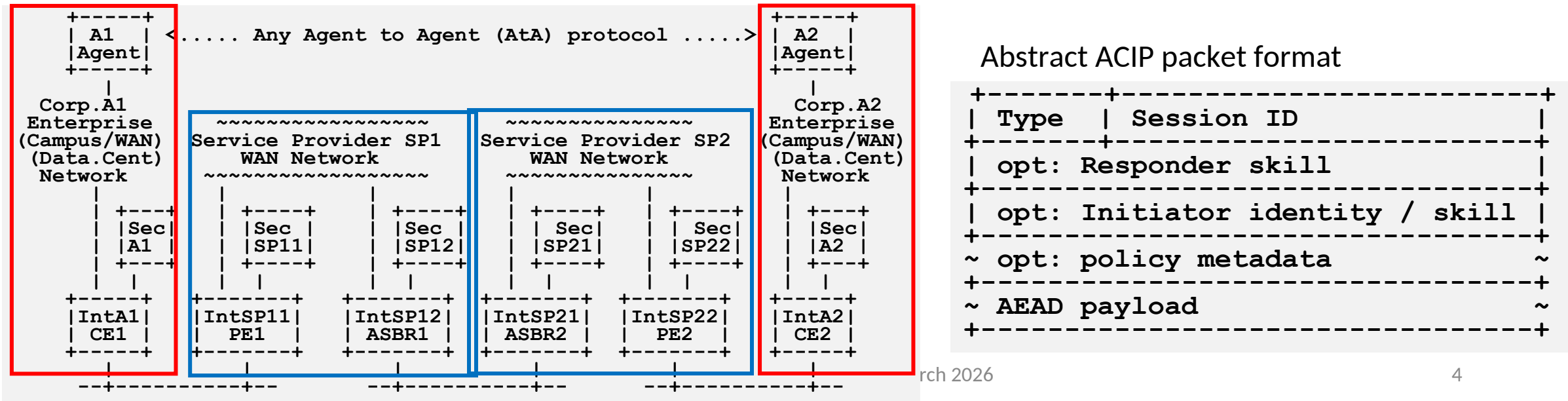
with existing technologies ... and (only) Internet - and cloud

- FinTech use cases. Evolve from HTTP B2B protocols to A2A
 - Banks, ATM operators, payment systems, Apps, PoS/Merchants, ...
- Security, Observability, Regulations, path routing compliance, resource guarantees,
- Outsourcing of responsibility to trusted parties (operators)....



Technical *current solution idea* summary overview

- ACIP: ‘name’ = (Agent) id/skill/task (“address”) based datagram layer (encrypted)
 - ACIP layer functions: route/load-split, police, filter, log/stat, replicate (multicast)
 - Datagram/Transaction AND connection support
 - ACIP session setup for high-speed A2A data transfers
 - Ideally inband in high-speed network equipment “IntXXX” service layer processing
 - Or-else integrate with OTT ‘security overlay’ nodes (example)
 - Control plane to register/distribute ‘skills’ Agent/ACIP-node, inter-ACIP-nodes
 - Re-using existing protocols where feasible (e.g.: new BGP AF for skills).



IETF work considerations

- What work might be done in the IETF?
 - New protocol: Specify ACIP protocol/functionality
 - Extensions to existing protocols: Control Plane, e.g.: BGP, HTTP?
- Where in the IETF might the work be done?
 - ACIP:
 - Area: INT/RTG. *Logically INT, but HW-forwarding experient in RTG (similar to multicast)*
 - Existing WG ? INTarea ? New WG (experimental – see LISP/BIER as examples).
 - Leverage lessons from ICNRG?!
 - Name = skilled based routing/registration/policies. No in-network caching though.
 - Abstract/leverage/reuse tenets of HTTP/URL processing on intermediate nodes
 - Existing WGs for control plane, whenever applicable

Work to date and future plans

- Where ?
 - Using “Enterprise” series of side-meetings (enterprise@ietf.org)
 - IETF124 Internet of Agents at Enterprises Side-Meeting (IoA@Enterprise)
 - <https://github.com/Enterprise-Network-protocol/Enterprise-Network/tree/main/ietf124-IoA%40Enterprise>
 - IETF125: IoA@Enterprise, Side Meeting thursday 18:00 - 19:30 Hunan
 - Security: AI agent security, Side meeting thursday 11:15 - 12:15 Hunan
- Work Focus / Goals
 - (1) Create AI service offerings for trusted network operator**
 - confidential/authenticated skill based routing, load-balancing, observation, policing / guardrails
 - ACIP is new underlay for A2A traffic, agnostic to A2A protocol
 - ACIP is new overlay service for private network service offerings
 - (2) Enable (optional) inband processing on high-speed/scale networking equipment**
 - (3) Reuse/expand proven IETF technologies (especially INT/RTG)**

Everything else happily taken from other solutions / proposals

AI Security: safe adoption, proactive defense

ADVERTISEMENT

draft-ni-a2a-ai-agent-security-requirements - *not specific to ACIP but for all agent solutions*

Example attack areas worrisome for agents

- **Blast Radius amplification**— via agents authorizations (OS CLI, email, social platform, “real world access”)
 - Example: agent auth phishing: **ClawJacked CVE-2026-25253** [OWASP TOP10 for Agentic Applications](#)
ASI-03 Id. & Priv Abuse, ASI-02 Tool Misuse, ASI-05 Unexpected Code Execution (RCE)
- **Semantic attacks** — Threat is in the payload/prompt, not only structural in header/encoding
- **Coarse/low security/authorizations**— Human authorizations passed to agents -> insufficient guardrails

Working Groups NO COORDINATION	AI Agent related work items / areas
RATS/SCITT	Security Management: Adopt “AI-BOM”, Attestation, Behavioral Benchmarking, Auditability
OAUTH/WIMSE/SCIM	Independent Identity Management: Assign independent identity to agents for specialized authorization
OAUTH/WIMSE	In-depth Authorization: Batch/workflow authorization BCP, security context preservation, consistent security policies, additional authz models, user-OBO-authorization-servers...
OPS AWG ?!	Visibility: Full observability to requests, abnormal inference resource usage, abnormal tool usage
IPSECME/TLS/./ANIMA	Transport Path Security: IPSEC, (D)TLS/QUIC, ACP, ‘VPN’, ...
?	In-time Response: Microsegmentation, identity/privilege revocation

Credit: Thanks to discussion on A2A list, catalyst list, SAAG, new works in hackathon, ..., including but not limited to: Peter, Usama, Henk, Arnaud, Orié, Brian, Dan...

Extending Discussion: Thursday 11:15-12:15 AI Agent Security Side Meeting @Hunan Room