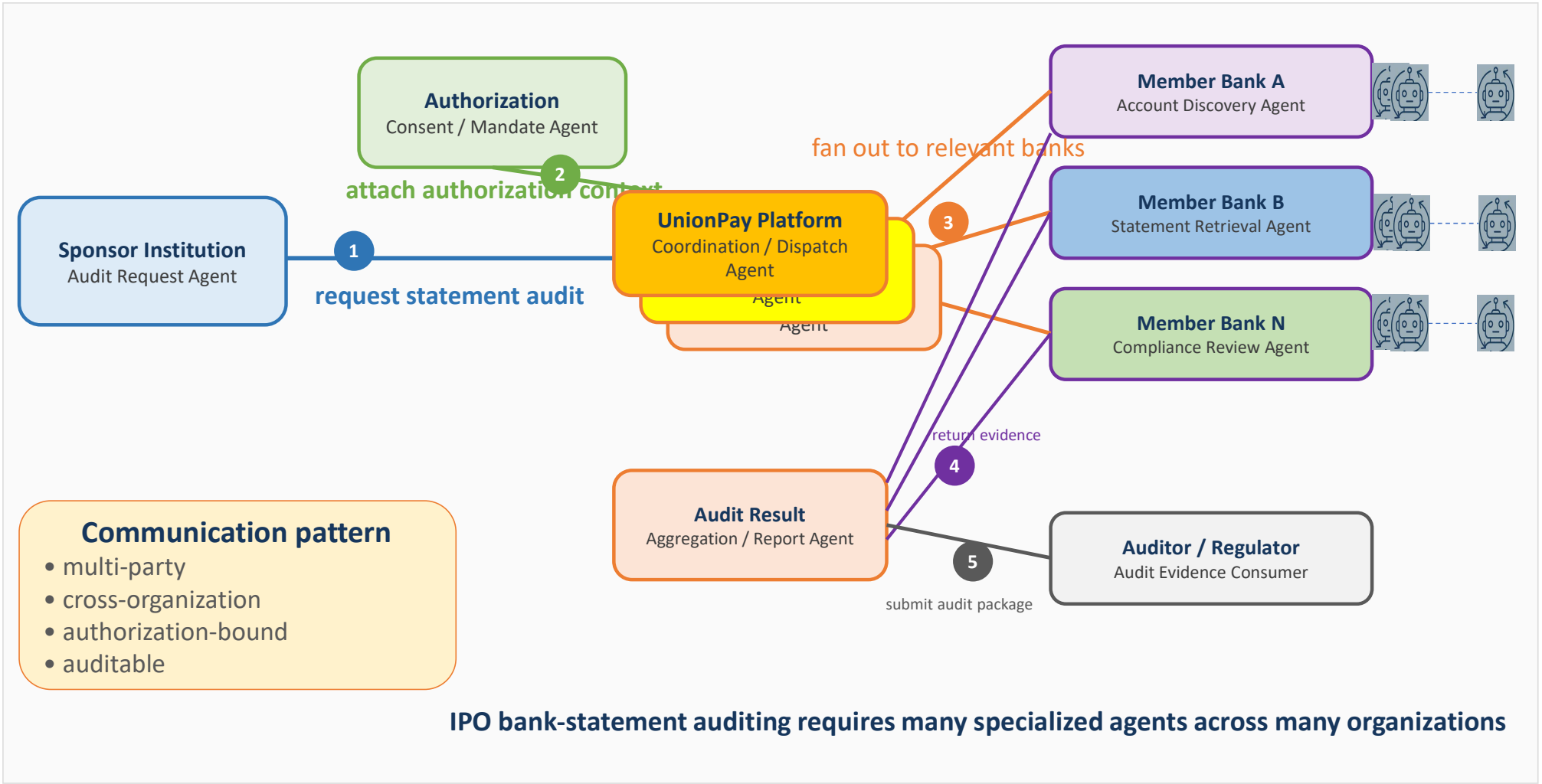
Deployment Scenarios, Gap Analysis, Requirement

draft-dunbar-dmsc-gw-scenarios-gap-analysis-02

L. Dunbar (Futurewei)
Y. Wang (China Telecom)
Bing Liu (Huawei)
July 2026

Key Question: What Agent GW is and is NOT; When it is needed; Key Properties

Use Case 1: UnionPay IPO Auditing



UnionPay Use Case: What the Communication Pattern Exposes

Direct A2A / Agent Cards do not answer consistently

Agent admission
Is the agent approved, active, compliant, and owned by the claimed organization?

Visibility control
Should this sponsor, merchant, or auditor see this capability at all?

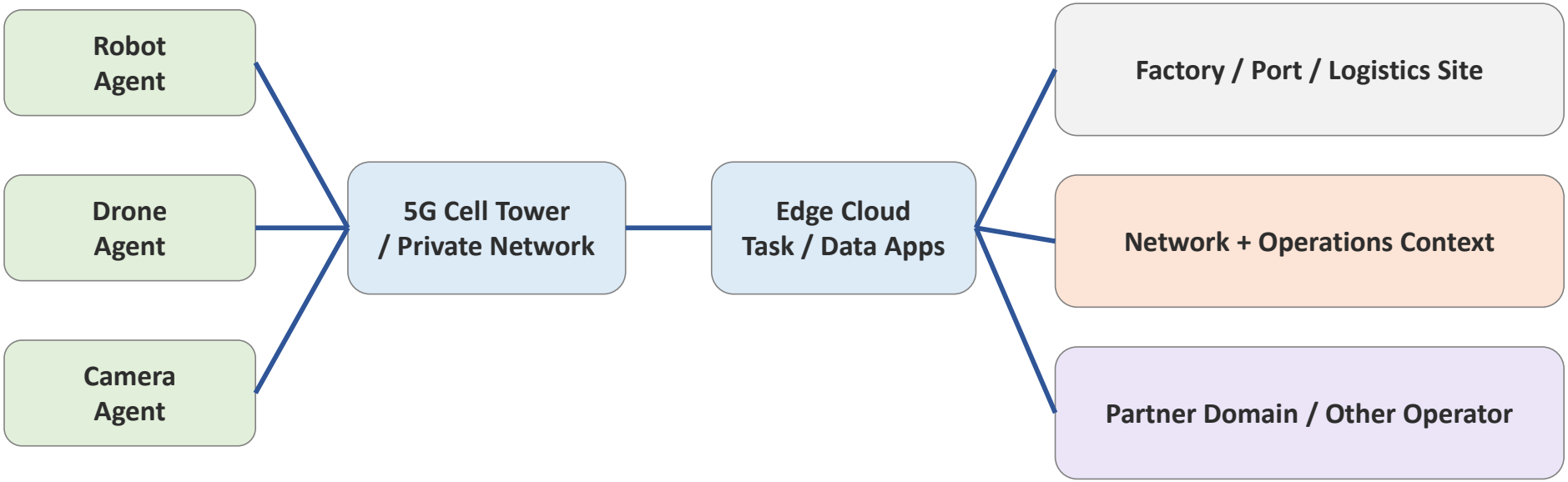
Authorization context
Is the request bound to the correct mandate, business purpose, and institution?

Cross-org audit
Can the trail span banks, sponsor, UnionPay, and regulator without custom pairwise integration?

Takeaway: the use case needs a managed control point for onboarding, selective exposure, authorization-bound routing, and audit — before thousands of institutions can interoperate.

Use Case 2: Telecom Operator Networks

Embodied AI agents in factories, ports, and logistics



Agent functions involved

Device onboarding, task dispatch, capability discovery, mobility tracking, action authorization, and cross-domain handoff
Communication pattern is not simple point-to-point: many devices, changing network attachment, and possible handoff to another domain

Two net-new requirements:

Network-aware mobility
Physical-world action authorization

Why This Use Case Exposes the Need for Gateway Functions

Direct A2A alone does not answer the operational questions

Multi-Vendor Campus	Mobility Across Cells / Edge	High-Risk Physical Action	Cross-Domain Handoff
Communication pattern	**Communication pattern**	**Communication pattern**	**Communication pattern**
Different devices and vendors	Location, edge, and QoS change	Drone / robot action has physical consequence	Task may continue in another operator domain
Function exposed by the use case	**Function exposed by the use case**	**Function exposed by the use case**	**Function exposed by the use case**
Need common onboarding, identity, and policy enforcement	Need current network context for selection and routing	Need per-action checks: zone, time, approval, risk	Need coordination and audit across domains

Takeaway: the telecom use case needs more than communication — it needs common onboarding, mobility-aware routing, action-level authorization, and cross-domain coordination.

What Properties Do These Use Cases Expose?

UnionPay / Financial Ecosystem	Telecom / Embodied AI
Cross-organization trust binding	Network-aware mobility
Policy-controlled capability visibility	Physical-world action authorization
Authorization-bound routing	Group / stream coordination
Cross-institution audit	Cross-domain handoff

What an AI Agent Gateway Is — and Is Not

A control and coordination layer around agent communication — not a replacement for agent protocols

✓ IS

Onboarding & Trust Binding
verified ownership, lifecycle, org identity

Policy Controlled Exposure
selective visibility; tenant / requester context

Physical-World Action Authorization
spatial, time, approval checks

Network-Aware Mobility
attachment, edge, slice/QoS state

Group & Stream Coordination
multi-party anchor; stream fan-out

Mediation & Handoff Resolution
intent, policy, constraints, failure reasons

Observability & Audit
routing, authorization, lifecycle events

✕ IS NOT

Not a replacement	for A2A, MCP, Agent Cards, or other agent protocols
Not just a proxy	more than message relay or API forwarding
Not an agent runtime	does not define model behavior, planning, or reasoning
Not universal taxonomy	does not standardize every AI-agent term or use case
Not always required	small single-domain direct interactions may not need it

When It's Needed:

A single agent calling a known peer may work fine with direct A2A + tokens.

Gateway value appears when deployments become multi-vendor, multi-tenant, cross-organization, mobile, or physically consequential. The same reason API gateways emerge once an org manages many APIs.

Gap Analysis: Possible DMSC Work

Use cases expose gateway-specific properties that may need interoperable behavior

Key Agent Gateway Properties

Onboarding & Trust Binding
verified ownership, lifecycle, org identity

Policy Controlled Exposure
selective visibility; tenant / requester context

Physical-World Action Authorization
spatial, time, approval checks

Network-Aware Mobility
attachment, edge, slice/QoS state

Group & Stream Coordination
multi-party anchor; stream fan-out

Mediation & Handoff Resolution
intent, policy, constraints, failure reasons

Observability & Audit
routing, authorization, lifecycle events

Interop gaps

Possible DMSC Work: Gateway-Facing Requirements / Models

1. Anchoring and Attaching to GW
common onboarding / lifecycle / health state
bind interactions to org identity + authorization context

2. Policy-Controlled Exposure
requester-specific capability visibility
tenant isolation and policy-aware routing

3. Mobility + Action Context
network context: attachment, edge, slice/QoS
action constraints: location, time, human approval, risk

4. Coordination + Audit
group / stream coordination and constrained handoff
gateway audit events: routing, authz, cross-domain

5. GW to GW Sync Protocol: capability dist., reachability updates, auth context, correlated audit

Goal for DMSC: identify which Gateway functions require interoperable specifications vs. local implementation or other venues.

Questions

- Are the deployment scenarios clear enough to evaluate the gateway problem?
- Are there important deployment scenarios missing, especially outside the presented operator/enterprise examples?
- More?