AgentFacts: Verified Metadata Infrastructure for AI Agent Commerce and Coordination

Jared James Grogan, Universitas AI
jared.grogan@post.harvard.edu
https://www.AgentFacts.org | github.com/jaredgrogan/agentfacts_standard

Abstract

Deployment of autonomous AI faces a critical "Know Your Agent" problem: organizations cannot reliably verify third-party agent capabilities, creating trust gaps that limit adoption. AgentFacts solves this through cryptographically-verified metadata—transforming agent capabilities from marketing claims into independently validated facts. AgentFacts provides ready-made regulatory compliance while simultaneously unlocking autonomous agent commerce capabilities through ten verified metadata categories that enable both automated AI compliance and agent-to-agent commerce. Like nutrition facts for food, AgentFacts provides standardized transparency that enables informed decisions across stakeholders while unlocking trillion-dollar agent economy potential through verified marketplace coordination.

1. The Know Your Agent Challenge

The emerging agent economy represents a trillion-dollar opportunity [1], yet realization requires solving fundamental trust infrastructure challenges. Current agent coordination approaches assume pre-existing trust within enterprise environments—functioning as "intranet-scale" solutions insufficient for cross-organizational commerce and coordination of autonomous agents. This paper presents the commerce-enabled AgentFacts standard, building on the foundational KYA framework [2] and implementation guide [3]. Future work will address specialized topics including comprehensive security analysis and agent economy dynamics.

The Core Problem: Organizations cannot confidently adopt third-party agents because capabilities remain unverifiable marketing claims rather than independently validated facts. This creates a coordination failure preventing the network effects necessary for agent marketplace development.

Current Limitations: Self-declared metadata lacks verification, centralized registries create single points of failure, and custom integration requirements don't scale across organizational boundaries.

AgentFacts Solution: A universal "Know Your Agent" standard that transforms agent metadata from unverifiable assertions into cryptographically-verified facts through multi-authority validation [2]. Like how Know Your Customer (KYC) enabled financial services coordination, AgentFacts provides the trust infrastructure for confident cross-organizational agent adoption.

2. Universal Ten-Category Schema

AgentFacts employs a comprehensive metadata architecture encompassing ten categories that enable both internal governance and external marketplace coordination [2]:

1. Core Identity: Unique identification using decentralized identifiers (DIDs), human-readable names, and version management with time-to-live freshness controls.

2. Baseline Model: AI foundation transparency including provider, training data sources, fine-tuning specifications, bias assessments, and safety evaluations for regulatory compliance.

3. Classification: Universal categorization by agent type (assistant/autonomous/tool/workflow), operational level (ambient/supervised/autonomous), and deployment context (enterprise/consumer/government).

4. Capabilities: Extensible capability declarations including APIs, tool protocols, programming languages, domain expertise, **plus commerce enablement**: payment protocols, pricing models, and spending authority specifications.

5. Authentication & Dynamic Permissions: Time-limited access control with permission authorities, escalation policies, audit trails, **and financial governance**: spending authority verification and payment authorization levels.

6. Compliance & Regulatory: Multi-jurisdictional markers for EU AI Act, NIST AI RMF, GDPR, and sector standards with automated compliance documentation generation.

7. Performance & Reputation: Measurable metrics including latency, availability, accuracy, user satisfaction, **plus commerce reliability**: transaction success rates, payment processing speed, and marketplace reputation scores.

8. Supply Chain: Component transparency through Software Bill of Materials (SBOM) integration covering dependencies, data sources, infrastructure providers, and security assessments.

9. Verification: Multi-authority cryptographic signatures from specialized validators—cybersecurity firms for security capabilities, compliance consultancies for regulatory adherence, performance organizations for operational metrics.

10. Programmability: Extension mechanisms for custom metadata, integration hooks, and backward compatibility ensuring future-proof implementations.

```
  "core_identity": {},
  "baseline_model": {},
  "classification": {},
  "capabilities": {},
  "authentication_permissions": {},
  "compliance_regulatory": {},
  "performance_reputation": {},
  "supply_chain": {},
  "verification": {},
  "extensibility": {}
}
```

Figure 1. AgentFacts Schema Overview (Simplified JSON Structure)

2.1 Multi-Authority Trust Model

Rather than relying on single verification sources, AgentFacts enables distributed trust through specialized authorities validating their domains of expertise. This eliminates single points of failure while enabling graduated confidence assessment based on verification authority reputation and track record.

AgentFacts defends against agent capability spoofing, compliance fraud, financial authority fraud, supply chain obfuscation, reputation manipulation, and coordination attacks through cryptographic verification and multi-authority validation. As a gatekeeper framework, AgentFacts enables systems to require verified metadata for participation, preventing malicious actors from entering agent marketplaces and coordination networks.

2.2 Commerce Infrastructure Integration

The schema transforms agents from internal tools into autonomous economic actors by incorporating verified financial metadata. Agents can assert payment capabilities, spending authorities, and transaction policies, enabling marketplace discovery and autonomous procurement within organizational controls. This autonomous commerce capability represents a fundamental advancement beyond trust-only agent standards, transforming agents from managed tools into autonomous economic actors with verified financial authority. Unlike traditional e-commerce where agents might book services or purchase products, agent-to-agent commerce enables computational marketplaces where agents buy and sell AI capabilities directly. An agent might purchase language translation from one provider, image processing from another, and data analysis from a third, composing complex workflows through verified marketplace coordination. This inference economy requires metadata that enables capability discovery, quality assessment, and autonomous procurement of AI services—transforming agent coordination from manual integration into programmable economic relationships. AgentFacts integrates with confidential computing infrastructure to protect sensitive agent interactions. Through Trusted Execution Environment (TEE) support, agents can engage in marketplace transactions without exposing proprietary prompts, business logic, or query patterns to service providers. This confidential

agent commerce ensures organizations can participate in agent economies while maintaining competitive intelligence and regulatory compliance.

2.3 Agent Discovery & Peer-to-Peer Coordination

AgentFacts enables decentralized agent discovery through metadata-based search without centralized registries. Agents discover compatible services through capability filtering, verify compliance status, and assess reputation scores before initiating coordination. This peer-to-peer architecture eliminates platform dependencies while maintaining verification integrity. Commerce metadata enables agents to discover payment-compatible services, verify spending authority, and negotiate transaction terms autonomously. Unlike existing frameworks requiring manual procurement approval, AgentFacts transforms agent-to-agent transactions into standardized marketplace interactions with cryptographic audit trails and automated compliance monitoring.

3. Implementation & Enterprise Value

AgentFacts leverages W3C Verifiable Credentials infrastructure for immediate deployment without custom cryptographic implementation. Verification authorities issue specialized credentials using standard DID-based signatures, while organizations verify using existing VC libraries across programming languages. This approach enables immediate implementation through proven cryptographic infrastructure without ecosystem development delays.

3.1 Concrete Example:

A financial services firm contracts an AI provider for regulatory reporting. The provider supplies AgentFacts metadata with verified baseline model information, compliance certifications from regulatory consultants, and security validation from cybersecurity firms. The enterprise evaluates these verified facts, assigns organizational roles through additional metadata layers, and implements dynamic permissions for quarterly reporting with automatic privilege adjustment based on operational context.

3.2 Enterprise Benefits

Governance Automation: Standardized compliance implementation for AI deployment and integrations reduces regulatory burden through automated documentation generation and multi-jurisdictional alignment, particularly valuable as AI regulations expand globally.

Financial Infrastructure: Verified spending authority enables autonomous agent procurement within corporate controls. Agents can discover services, verify pricing, and execute transactions with automated compliance monitoring and audit trail generation.

Risk Management: Supply chain transparency through SBOM integration provides security and compliance visibility across agent dependencies, essential for enterprise risk assessment.

Competitive Advantage: Organizations participate in agent marketplaces without compromising competitive intelligence through selective metadata disclosure and confidential computing integration.

Commerce Transformation: The standard commerce-enabled metadata fields distinguish AgentFacts from existing trust-only standards, enabling autonomous agent procurement that reduces manual oversight while maintaining financial governance, confidentiality, and security. Agents can discover payment-compatible services, verify spending authority, and execute transactions within predetermined organizational controls—transforming isolated agent deployments into interconnected commerce ecosystems.

3.3 Adoption Pathway

Implementation begins with internal coordination—adding metadata labels to existing agents for improved governance and resource allocation. This provides immediate value while ensuring compliance automation with the EU AI Act for EU exposed companies and operational transparency [3].

As verification authorities establish market presence, organizations progressively adopt multi-authority validation for external coordination. The Apache 2.0 license ensures vendor neutrality without licensing friction.

3.4 Network Effects

Early adopters benefit from internal coordination improvements. As adoption expands, network effects emerge: broader agent ecosystems, reduced integration complexity, standardized marketplace interactions, and enhanced coordination capabilities across organizational boundaries.

4. Conclusion

AgentFacts establishes the foundational trust infrastructure necessary for the trillion-dollar agent economy through verified metadata that transforms agent capabilities from marketing claims into independently validated facts. The ten-category schema provides comprehensive agent characterization while W3C Verifiable Credentials integration enables immediate deployment. Multi-authority verification eliminates single points of trust failure while commerce infrastructure transforms agents into autonomous marketplace participants.

As vendor-neutral internet infrastructure, AgentFacts enables "TCP/IP for agent interactions"—providing the semantic trust layer that existing operational protocols require for secure internet-scale coordination. This positions agent procurement as standardized organizational resource management rather than bespoke integration projects, unlocking confident AI deployment at scale. This extends the foundational KYA framework [2] with autonomous commerce capabilities detailed in the companion enterprise implementation guide [3].

Available Now: Complete specification and reference implementations at AgentFacts.org with open-source development at github.com/jaredgrogan/agentfacts_standard under Apache 2.0 license.

References:

[1] Grady, P., Huang, S., and Buhler, K. "AI's Trillion-Dollar Opportunity: Sequoia AI Ascent 2025 Keynote." Inference by Sequoia Capital, May 7, 2025. https://inferencebysequoia.substack.com/p/ais-trillion-dollar-opportunity-sequoia

[2] Grogan, J. J. (2025). AgentFacts: Universal KYA Standard for Verified AI Agent Metadata & Deployment. arXiv preprint arXiv:2506.13794.

[3] Grogan, J. J. (2025). Implementing AgentFacts at Enterprise Scale: Verified Metadata for Secure AI Deployment & Discovery. arXiv preprint.

Appendix A. - AgentFacts JSON Schema Specification

```
{
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "$id": "https://agentfacts.org/schemas/v1/agentfacts-core-v1.json",
 "title": "AgentFacts Universal Metadata Standard v1.0",
 "description": "Core metadata structure for verified AI agent coordination and commerce",
 "type": "object",
 "required": ["core_identity", "baseline_model"],
 "properties": {
  "core_identity": {
   "type": "object",
   "description": "REQUIRED: Unique agent identification and lifecycle metadata",
   "properties": {
    "agent_id": {"type": "string"},
    "agent_name": {"type": "string"},
    "version": {"type": "string"},
    "created_timestamp": {"type": "string"},
    "ttl_hours": {"type": "integer"}
   }
  },
  "baseline_model": {
   "type": "object",
   "description": "REQUIRED: Foundation AI model transparency",
   "properties": {
    "provider": {"type": "string"},
    "model_family": {"type": "string"},
    "training_data_sources": {"type": "array"},
    "fine_tuning_specs": {"type": "object"},
    "safety_evaluations": {"type": "array"}
   }
  },
  "classification": {
   "type": "object",
   "description": "Universal categorization system",
   "properties": {
    "agent_type": {"enum": ["assistant", "autonomous", "tool", "workflow"]},
    "operational_level": {"enum": ["ambient", "supervised", "autonomous"]},
    "deployment_context": {"enum": ["enterprise", "consumer", "government"]},
    "risk_classification": {"enum": ["low", "medium", "high", "critical"]}
   }
  },
  "capabilities": {
   "type": "object",
   "description": "Extensible capability declarations including commerce",
   "properties": {
```

```
      "supported_apis": {"type": "array"},
      "confidential_endpoints": {"type": "array", "description": "TEE-protected API endpoints for
privacy-preserving interactions"},
      "tool_protocols": {"type": "array"},
      "programming_languages": {"type": "array"},
      "domain_expertise": {"type": "array"},
      "payment_protocols": {"type": "array", "description": "Supported payment standards
[stripe|ethereum|lightning|agent_credits|paypal]"},
      "payment_acceptance": {"type": "boolean", "description": "Flag indicating payment
capability for quick discovery"},
      "payment_endpoint": {"type": "string", "description": "Universal payment routing address
(agent-pay:// scheme)"},
      "pricing_models": {"type": "array", "description": "Business models
[per_query|hourly|subscription|success_fee|flat_rate]"},
      "payment_interfaces": {"type": "array", "description": "Payment interactions
[direct_transfer|escrow|marketplace|subscription]"},
      "commerce_enabled": {"type": "boolean", "description": "Quick discovery flag for
commerce scenarios"},
      "commerce_capabilities": {"type": "object"}
    }
  },
  "authentication_permissions": {
    "type": "object",
    "description": "Dynamic access control and financial governance",
    "properties": {
      "supported_auth_methods": {"type": "array"},
      "current_permissions": {"type": "array"},
      "permission_scope": {"type": "string"},
      "permission_ttl": {"type": "string"},
      "spending_authority": {"type": "object", "description": "Autonomous purchasing limits and
controls"},
      "payment_authorization_level": {"type": "string"},
      "financial_governance": {"type": "object"}
    }
  },
  "compliance_regulatory": {
    "type": "object",
    "description": "Multi-jurisdictional regulatory compliance",
    "properties": {
      "eu_ai_act_compliance": {"type": "string"},
      "nist_ai_rmf_alignment": {"type": "string"},
      "gdpr_compliance": {"type": "boolean"},
      "sector_standards": {"type": "array"},
      "geographic_compliance": {"type": "array"},
      "audit_certifications": {"type": "array"},
      "payment_compliance": {"type": "object", "description": "Financial compliance for agentic
```

commerce"},
"aml_kyc_status": {"enum": ["verified", "pending", "not_required"], "description": "Anti-money laundering status"},
"tax_jurisdiction": {"type": "string", "description": "Primary tax reporting jurisdiction [US|EU|UK|CA]"},
"payment_licenses": {"type": "array", "description": "Processing authorizations [money_transmitter|processor_registration|exempt]"},
"commerce_compliance_score": {"type": "number", "description": "Aggregate financial rating (0.0-10.0 scale)"}
}
},
"performance_reputation": {
"type": "object",
"description": "Quality metrics including commerce reliability",
"properties": {
"response_time_p50": {"type": "number"},
"availability_sla": {"type": "number"},
"accuracy_metrics": {"type": "object"},
"user_satisfaction": {"type": "number"},
"commerce_reputation_score": {"type": "number", "description": "Agent-to-agent satisfaction rating (0.0-5.0)"},
"transaction_success_rate": {"type": "number", "description": "Financial transaction completion rate (0.0-100.0)"},
"payment_processing_speed": {"type": "number"},
"payment_reliability_score": {"type": "number", "description": "Payment system uptime percentage (0.0-100.0)"},
"payment_dispute_rate": {"type": "number", "description": "Transaction dispute percentage (0.0-100.0)"},
"spending_accuracy": {"type": "number", "description": "Budget adherence percentage (0.0-100.0)"},
"commerce_volume": {"enum": ["enterprise", "high", "medium", "low"], "description": "Abstracted volume classification"}
}
},
"supply_chain": {
"type": "object",
"description": "SBOM integration for transparency",
"properties": {
"component_dependencies": {"type": "array"},
"data_sources": {"type": "array"},
"infrastructure_providers": {"type": "array"},
"security_assessments": {"type": "array"},
"license_compliance": {"type": "object"}
}
},
"verification": {

```
      "type": "object",
      "description": "Multi-authority cryptographic validation",
      "properties": {
        "verification_authorities": {"type": "array"},
        "cryptographic_signatures": {"type": "array"},
        "confidence_levels": {"type": "object"},
        "verification_timestamp": {"type": "string"},
        "trust_policies": {"type": "object"}
      }
    },
    "programmability": {
      "type": "object",
      "description": "Extension mechanisms and future-proofing",
      "properties": {
        "custom_extensions": {"type": "object"},
        "integration_hooks": {"type": "array"},
        "schema_version_compatibility": {"type": "string"},
        "backward_compatibility": {"type": "boolean"}
      }
    }
  },
  "additionalProperties": true
}
```