BRIEF DESCRIPTION OF THE DRAWINGS

MULTI-DOMAIN AUTHENTICATION AND AUTHORIZATION SYSTEM WITH CREDENTIAL PORTABILITY FOR AI AGENT NETWORKS

FIGURE 1 - System Architecture Overview

Figure 1 illustrates the complete system architecture 100 for multi-domain authentication of AI agent networks, showing:

- **Universal Identity Abstraction Layer (102):** Central component generating UIDs for AI agents (112) and human users (114)
- **Credential Translation Engine (104):** Converts between different credential types across domains
- **Behavioral Authentication Framework (106):** Continuously monitors and validates agent behavior
- **Trust Bridge Protocol Module (108):** Negotiates between domains with different trust models
- **Distributed Session Management (110):** Maintains sessions with Byzantine fault tolerance
- **Multiple Security Domains (116a, 116b, 116c):** Different environments with varying requirements
- **Central Controller (118):** Coordinates all authentication processes
- **Data flows:** Indicated by arrows showing credential flow, behavioral data, and session information

---

FIGURE 2 - Credential Translation Engine Detail

Figure 2 provides a detailed view of the Credential Translation Engine 200, illustrating:

- **Supported Credential Types (202-216):**
  - API Keys (202)
  - X.509 Certificates (204)
  - OAuth Tokens (206)
  - JWT Tokens (208)
  - SAML Assertions (210)
  - Kerberos Tickets (212)
  - Hardware Security Module Credentials (214)
  - Behavioral Authentication Patterns (216)
- **Secure Multiparty Computation Protocol (220):**
  - Source Domain Authority (222)

- Target Domain Authority (224)
- Neutral Translation Services (226)
- Threshold cryptography connections

- **Translation Process Flow:**
  - Input validation stage
  - Semantic mapping layer
  - Output generation stage
  - Audit trail creation

FIGURE 3 - Behavioral Authentication Framework

Figure 3 depicts the Behavioral Authentication Framework 300 components:

- **Behavioral Dimensions Analyzed:**
  - API Call Patterns (302): Sequence, frequency, parameters
  - Resource Consumption Patterns (304): CPU, memory, network, storage
  - Decision-Making Patterns (306): Classification, response selection
  - Interaction Sequences (308): Inter-agent communication
  - Temporal Patterns (310): Activity rhythms, burst behavior
- **Machine Learning Module (312):**
  - LSTM Networks for sequence analysis
  - Isolation Forest for anomaly detection
  - One-Class SVM for pattern recognition
  - Autoencoder for feature extraction
  - Ensemble voting mechanism
- **Comparison Engine (314):**
  - Baseline storage
  - Real-time comparison
  - Deviation calculation
  - Statistical analysis
- **Anomaly Response Module (316):**
  - Threshold evaluation
  - Response selection

- Alert generation
- Audit logging

FIGURE 4 - Trust Bridge Protocol

Figure 4 illustrates the Trust Bridge Protocol 400 operation:

- **Multi-Phase Negotiation Process (402):**
  - Discovery Phase (404): Exchange capabilities and requirements
  - Negotiation Phase (406): Find common authentication methods
  - Establishment Phase (408): Create cryptographic bindings
  - Maintenance Phase (410): Monitor and update relationships
- **Supported Trust Models:**
  - Hierarchical Trust/PKI (412): Certificate authorities, chain validation
  - Web of Trust (414): Peer relationships, reputation scoring
  - Blockchain-Based Trust (416): Distributed ledger, smart contracts
  - Zero-Knowledge Proof Systems (418): Privacy-preserving verification
- **Protocol Messages:**
  - Capability announcements
  - Requirement negotiations
  - Binding confirmations
  - Health check updates
- **Trust Level Elevation Path:** Shows progressive authentication flow

---

FIGURE 5 - Byzantine Fault Tolerant Session Management

Figure 5 shows the Distributed Session Management architecture 500:

- **Node Configuration:**
  - Primary Node (502)
  - Backup Nodes (504a-504f): Total of 7 nodes (3f+1 where f=2)
  - Failed/Byzantine Node indication (506)
- **Consensus Protocol Phases:**
  - REQUEST: Client to primary

    - PRE-PREPARE: Primary broadcasts
    - PREPARE: Inter-node agreement
    - COMMIT: Execution confirmation
    - REPLY: Client response
- **Session State Replication:**
    - State distribution arrows
    - Consistency verification
    - Update propagation
    - Conflict resolution
- **Message Flow Diagram:**
    - Normal operation path (solid lines)
    - View change path (dashed lines)
    - Fault detection indicators
    - Recovery mechanisms
- **Session Components Shown:**
    - Session ID management
    - Credential storage
    - Behavioral scores
    - Ephemeral keys
    - Replay counters

Additional Drawing Notes

All figures use the following conventions:

- **Solid lines:** Primary data/control flow
- **Dashed lines:** Alternative or conditional paths
- **Thick borders:** Security boundaries
- **Shaded areas:** Encrypted or protected zones
- **Numbered circles:** Process sequence indicators

Figures are drawn to USPTO standards:

- Black ink on white background

- No color or grayscale
- Clear labeling with reference numerals
- Consistent symbol usage throughout
- Suitable for reproduction at patent publication size

End of Drawings Description