

WFAP System Architecture

Wells Fargo Agent Protocol - Technical Documentation

Multi-Agent Financial Marketplace Design

Table of Contents

1. Executive Summary	3
2. System Overview Architecture	4
3. Agent Interaction Flow	5
4. Component Architecture	6
5. Data Flow & Message Structure	7
6. Security & Compliance Layer	8
7. Implementation Recommendations	9

1. Executive Summary

Project Overview

The Wells Fargo Agent Protocol (WFAP) represents a revolutionary approach to financial services automation, where AI agents act as intelligent CFOs for companies, automatically requesting and evaluating financial products from multiple banks in real-time.

System Objectives

- **Automated Financial Discovery:** Enable companies to automatically discover and evaluate financial products across multiple institutions
- **ESG Integration:** Incorporate environmental, social, and governance factors into financial decision-making
- **Regulatory Compliance:** Ensure full audit trails and compliance with financial regulations (DORA, MAS, Basel III)
- **Competitive Marketplace:** Create transparent competition among financial institutions
- **Risk Assessment Automation:** Automate credit evaluation and risk analysis processes

Key Innovation Areas

Technology Stack

- Multi-agent AI architecture
- Digital signature protocols
- Real-time message routing
- LLM-powered ESG analysis
- Blockchain audit trails

Business Value

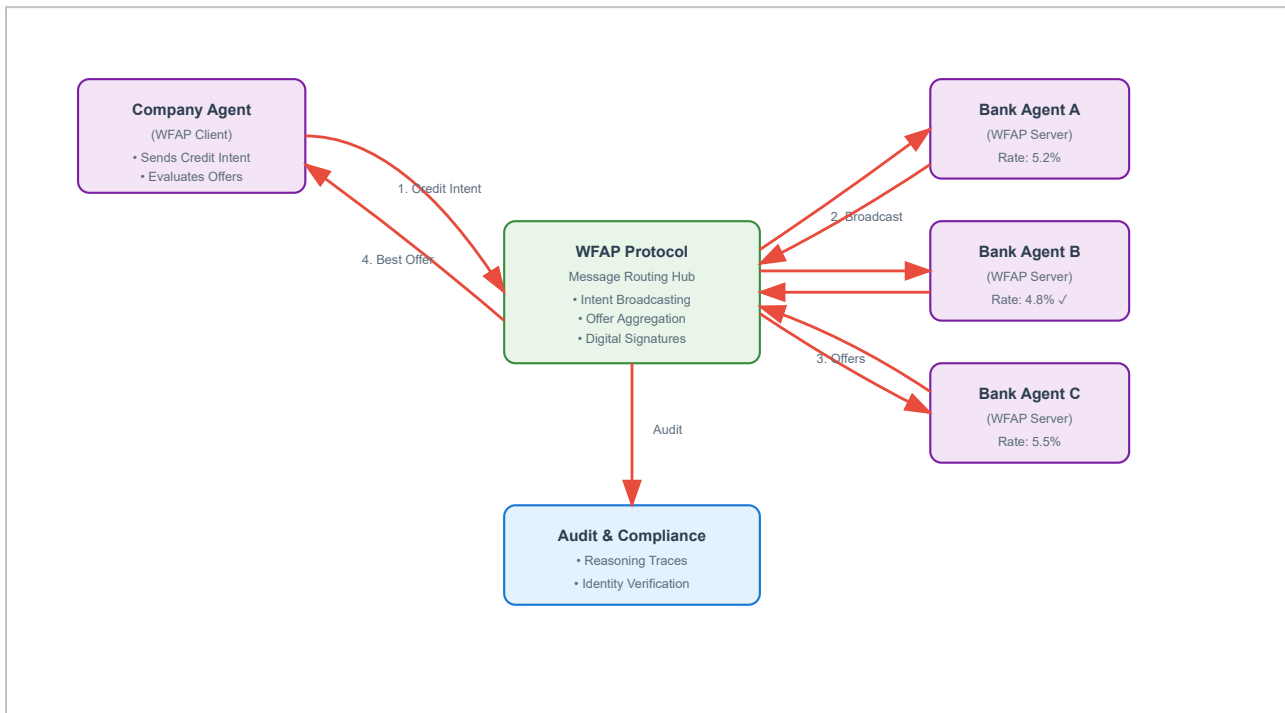
- Reduced transaction costs
- Faster credit processing
- Enhanced market transparency
- Improved ESG compliance
- Automated risk management

Core System Features

- **Agent-to-Agent Communication:** Standardized protocol for automated financial negotiations
- **Multi-Bank Competition:** Simultaneous evaluation of offers from multiple financial institutions
- **Carbon-Adjusted Pricing:** Integration of environmental factors into interest rate calculations
- **Comprehensive Audit Trails:** Complete reasoning and verification logs for regulatory compliance
- **Real-time Decision Making:** Automated offer evaluation and selection based on multiple criteria

2. System Overview Architecture

High-Level System Architecture



The system operates as a hub-and-spoke architecture where the WFAP protocol acts as the central message router, enabling secure communication between company agents seeking financial products and multiple bank agents offering competitive terms.

Architectural Principles

Design Patterns

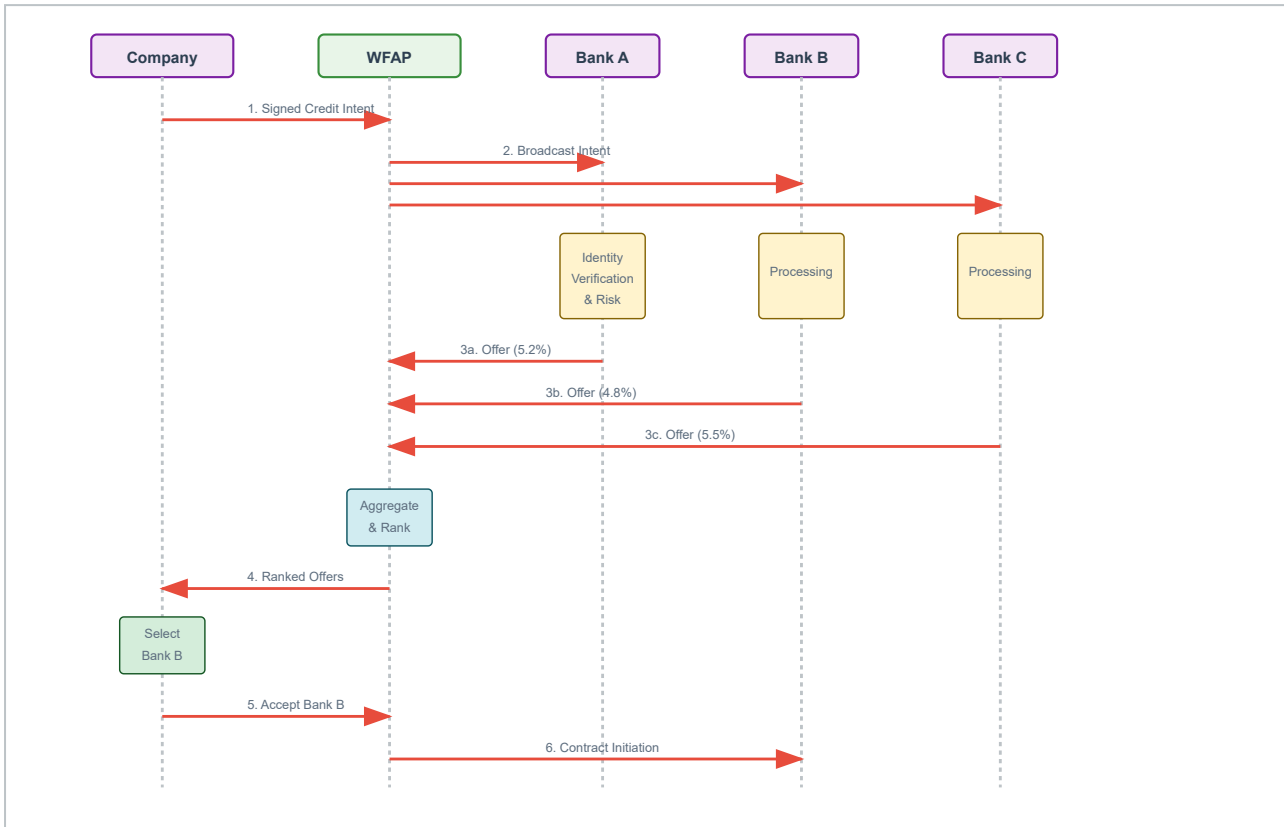
- Multi-agent system architecture
- Publisher-subscriber messaging
- Request-response with aggregation
- Event-driven processing

Quality Attributes

- Scalability: Horizontal agent scaling
- Security: End-to-end encryption
- Reliability: Fault-tolerant messaging
- Auditability: Complete trace logs

3. Agent Interaction Flow

Sequence Diagram - Complete Transaction Lifecycle



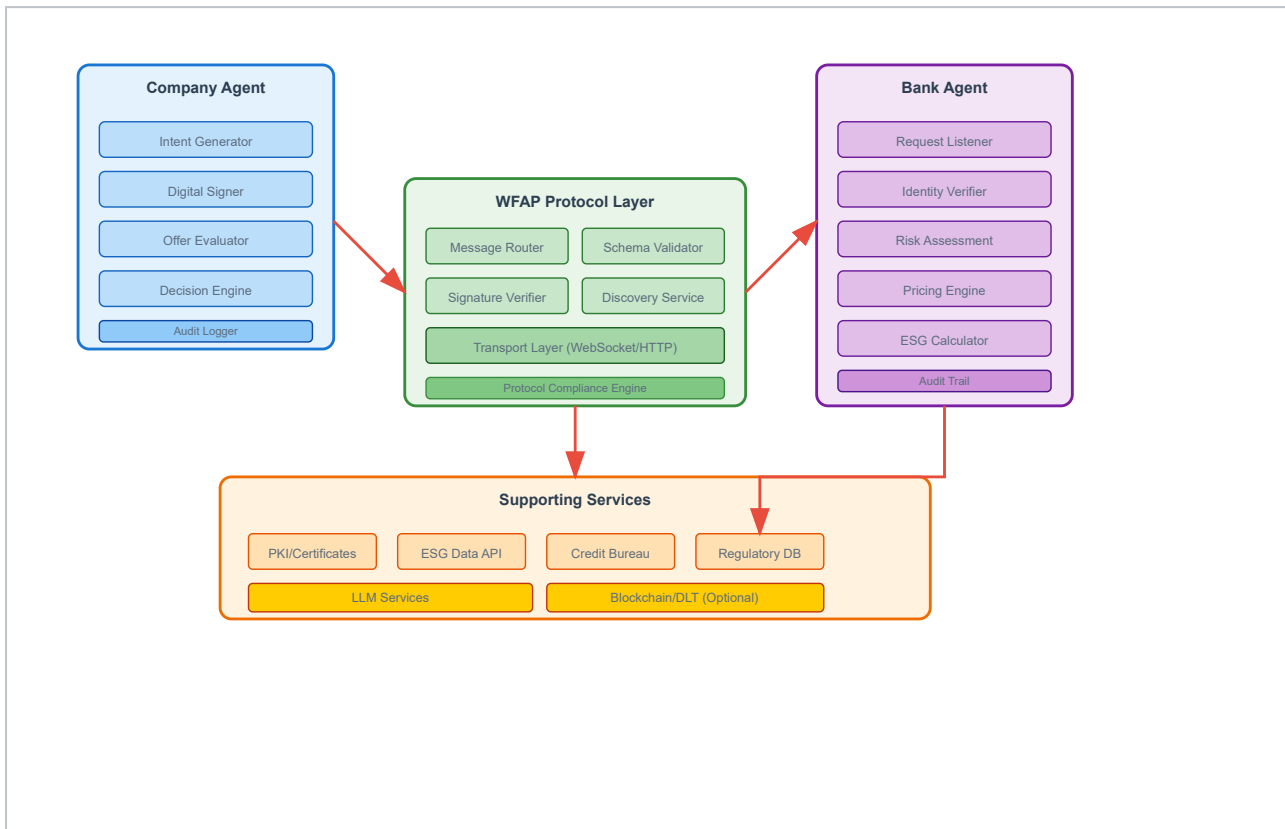
The interaction flow demonstrates the complete lifecycle from credit intent creation to contract initiation. Each bank agent independently processes requests and provides competitive offers, with the company agent automatically selecting the optimal solution based on predefined criteria.

Process Highlights

- **Parallel Processing:** Multiple banks evaluate requests simultaneously for faster response times
- **Digital Identity:** Cryptographic verification ensures authenticity at every step
- **Automated Ranking:** Multi-criteria decision making with ESG and financial factors
- **Audit Trail:** Complete transaction history for regulatory compliance
- **Real-time Negotiation:** Immediate offer evaluation and acceptance

4. Component Architecture

Detailed Component Structure



The component architecture illustrates the modular design of each agent type, with clear separation of concerns and well-defined interfaces. Supporting services provide shared functionality for security, compliance, and external data integration.

Component Responsibilities

Company Agent Components

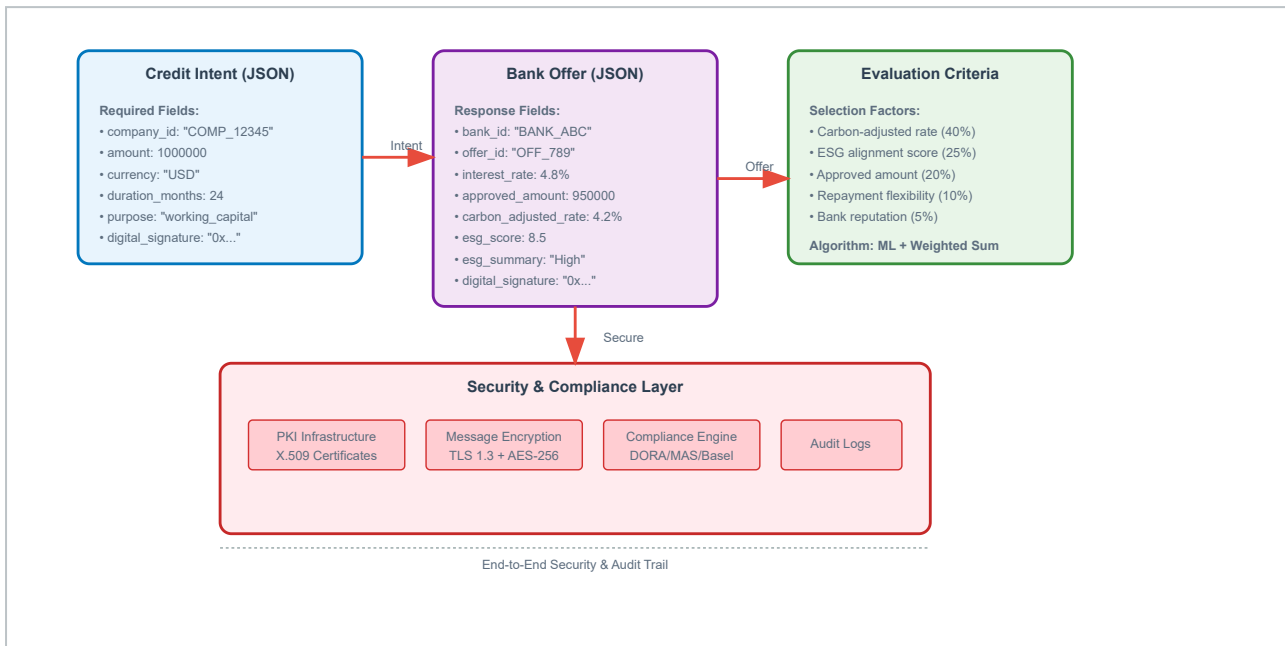
- **Intent Generator:** Creates structured credit requests
- **Digital Signer:** Cryptographic message signing
- **Offer Evaluator:** Multi-criteria offer analysis
- **Decision Engine:** Optimal offer selection

Bank Agent Components

- **Request Listener:** Incoming intent processing
- **Identity Verifier:** Customer authentication
- **Risk Assessment:** Credit evaluation engine
- **ESG Calculator:** Sustainability scoring

5. Data Flow & Message Structure

Message Structure and Data Flow



The data flow architecture ensures structured message exchange with comprehensive security and audit capabilities. JSON schemas define consistent data formats while cryptographic signatures ensure message integrity and authenticity.

Message Validation Schema

Intent Schema: Validates company identity, financial requirements, ESG preferences, and digital signatures.

Offer Schema: Ensures bank identification, pricing terms, ESG scores, regulatory compliance, and cryptographic authenticity.

Audit Schema: Captures decision reasoning, identity verification steps, and regulatory compliance evidence.

ESG Integration Framework

Environmental Factors

- Carbon footprint assessment
- Renewable energy usage
- Environmental impact scoring
- Green finance incentives

Social & Governance

- Social impact measurement
- Governance quality scores
- Ethical business practices
- Stakeholder engagement

6. Security & Compliance Layer

Identity & Authentication Framework

Digital Identity Management

PKI Infrastructure: X.509 certificates for agent identity verification with certificate revocation list (CRL) support.

Digital Signatures: ECDSA with SHA-256 for message authentication and non-repudiation.

OAuth 2.0 Integration: Token-based authentication for API access with JWT tokens for session management.

Regulatory Compliance

DORA Compliance

- Operational resilience testing
- Third-party risk management
- Incident reporting mechanisms
- Business continuity planning

MAS Guidelines

- FEAT principles assessment
- AI governance frameworks
- Risk management protocols
- Consumer protection measures

Audit Trail Architecture

Comprehensive Audit Logging

Identity Verification Traces: Complete logs of certificate validation, signature verification, and company registry lookups.

Risk Assessment Reasoning: Detailed records of credit scoring, industry risk analysis, and historical performance evaluation.

ESG Calculation Logs: Transparent records of environmental impact assessment, social scoring, and governance evaluation.

Decision Reasoning: Multi-criteria analysis logs, preference matching records, and optimization algorithm traces.

Data Protection & Privacy



Privacy-Preserving Technologies

- **Zero-Knowledge Proofs:** Verify credit scores above thresholds without revealing actual values
- **Homomorphic Encryption:** Perform calculations on encrypted financial data
- **Secure Multi-Party Computation:** Collaborative risk assessment without data sharing
- **Differential Privacy:** Statistical analysis while protecting individual privacy
- **Data Minimization:** Process only necessary information for decision making

Security Monitoring & Incident Response

Real-time Monitoring

- Anomaly detection systems
- Transaction pattern analysis
- Network traffic monitoring
- Agent behavior analysis

Incident Response

- Automated threat detection
- Incident escalation protocols
- Forensic analysis capabilities
- Recovery procedures

7. Implementation Recommendations

Technology Stack Recommendations

Backend Infrastructure

- **Runtime:** Node.js with TypeScript
- **Framework:** Express.js with WebSocket
- **Database:** PostgreSQL + Redis cache
- **Message Queue:** RabbitMQ/Apache Kafka
- **Container:** Docker with Kubernetes

AI/ML Components

- **LLM Integration:** OpenAI GPT-4/Claude API
- **ML Framework:** TensorFlow.js/PyTorch
- **Risk Models:** Scikit-learn/XGBoost
- **ESG Analysis:** Custom NLP models
- **Decision Engine:** Multi-criteria optimization

Testing & Validation Strategy

Functional Testing

- Unit tests for all components
- Integration tests for agent interactions
- End-to-end transaction testing
- Schema validation testing

Security Testing

- Digital signature verification
- Message integrity testing
- Authentication bypass testing
- Audit trail validation

Future Enhancements

Post-Hackathon Roadmap

Advanced Negotiations: Multi-round bidding with counter-offers and dynamic pricing adjustments.

Blockchain Integration: Immutable audit trails using distributed ledger technology for enhanced trust.

Regulatory Expansion: Support for additional jurisdictions (EU GDPR, US regulations, Asian markets).

Advanced Privacy: Implementation of homomorphic encryption and secure multi-party computation.

Market Intelligence: Real-time market data integration for dynamic pricing and risk assessment.



Success Metrics

- **Transaction Speed:** Complete credit evaluation in under 30 seconds
- **Accuracy:** 95%+ precision in risk assessment and ESG scoring
- **Compliance:** 100% audit trail completeness and regulatory adherence
- **Scalability:** Support for 1000+ concurrent agent interactions
- **Security:** Zero successful security breaches or data leaks

