JUL – Angola's National Logistics Single Window (Phase 1)
High-Level Design

DOCUMENT HISTORY & QUALITY CONTROL

Version	Date of Issue	Author	Summary Of Changes
1.0	December 2, 2025	Gracia Vijayan	Initial Template - Basic system architecture framework with core microservices design, preliminary technology stack selection, and foundational infrastructure requirements.
1.1	December 5, 2025	Linoy Pappachan Malakkaran	Enhanced Integration Layer - Added ASYCUDA integration specifications, SINTECE API definitions, initial security framework with Keycloak implementation, and basic deployment architecture.

1.2	December 9, 2025	Linoy Pappachan Malakkaran	Data Architecture Refinement - Implemented WCO Data Model Version 3.10 compliance, added master data management specifications, defined database-per-service pattern, and enhanced data flow diagrams.
1.3	December 12, 2025	Linoy Pappachan Malakkaran	Infrastructure Enhancement - Defined Kubernetes cluster architecture for three environments (Dev/Staging/Production), added network segmentation design, implemented monitoring stack with Prometheus/Grafana, and enhanced backup/recovery procedures.
1.4	December 15, 2025	Linoy Pappachan Malakkaran	Security & Compliance Update - Added Multi-Factor Authentication requirements, implemented TLS 1.3 encryption standards, defined network security zones (DMZ/Application/Data/Management), enhanced audit logging, and added WTO TFA compliance alignment.
2.0	December 17, 2025	Linoy Pappachan Malakkaran	Production Ready Release - Consolidated microservices architecture, upgraded technology stack (Angular 20+, ASP.NET Core 10.0, PostgreSQL 15+, Keycloak 23+), added Camunda 8 workflow engine and Kong API Gateway, implemented complete integration flows with SLA definitions, added 18 architectural diagrams, defined performance targets (99.9% uptime, <3s response, 100 TPS, 10K concurrent users), and comprehensive CI/CD pipeline with GitLab/ArgoCD.
2.1	December 22, 2025	Linoy Pappachan Malakkaran	Architectural diagrams added

Next Review Date:

Although this document is classified as FINAL, it is still subject to the Continuous Service Improvement process; therefore, it is not necessary to wait until the annual review date to make improvements.

Note: As this document is a controlled document, any updates or improvements must be implemented under strict change control via the process owner. All reviewers must review and approve all updates.

Document owner:

Role	Name
Document Owner	Ad Ports Technical Team
Deputy Document Owner	

Signatures

This document has been reviewed by:

Role	Name	Signature	Date
Manager - Architecture and Business Analysis	Indranil Majumder		

This document has been approved by:

Role	Name	Signature	Date
Manager - Architecture and Business Analysis	Indranil Majumder		

Table of Contents

1 Introduction

1.1 Purpose and Audience

This High-Level Design (HLD) document provides a comprehensive architectural blueprint for the JUL (Janela Única Logística) - Angola's National Logistics Single Window System. The document outlines the technical architecture, design decisions, and implementation approach for a modern, scalable trade facilitation platform.

The JUL system serves as a central hub for customs clearance and regulatory compliance, integrating multiple government agencies and private sector stakeholders to streamline trade processes, reduce clearance times, and enhance transparency in logistics operations.

Target Audience: This document is intended for technical architects, development teams, infrastructure engineers, project managers, business analysts, and stakeholders involved in the design, implementation, and operation of the JUL system.

Key Objectives:

- Provide single-point submission for trade-related documents
- Enable real-time tracking of shipments and cargo
- Facilitate seamless integration with customs and regulatory agencies
- Ensure compliance with World Customs Organization (WCO) standards
- Support concurrent users up to 10,000 with 99.9% system availability
- Process transactions with response time < 3 seconds (95th percentile)

1.2 Definitions, Acronyms and Abbreviations

Abbreviation/ Term	Description
AGT	Administração Geral Tributária (Angola Customs Authority)
ASYCUDA	Automated System for Customs Data (UN customs system)
CNCA	Certificado Nacional de Capacidade Aduaneira (National Customs Capacity Certificate)
CUSDEC	Customs Declaration Message (UN/EDIFACT)
CUSRES	Customs Response Message (UN/EDIFACT)
DU	Declaração Única (Single Declaration for customs)
HS	Harmonized System (commodity classification)
JUL	Janela Única Logística (Angola National Logistics Single Window)
OGA	Other Government Agencies
SINTECE	Sistema Nacional de Troca Electrónica de Dados (Angola Single Window)
WCO	World Customs Organization
WTO TFA	World Trade Organization Trade Facilitation Agreement

1.3 References

- JUL-AGT Integration Control Document - Draft - V2 (ASYCUDA integration specifications)
- JUL-SINTECE Integration Control Document - Draft - v2 (SINTECE integration specifications)

- JUL System User Management Architecture (Keycloak implementation details)
- WCO Data Model Version 3.10 (World Customs Organization standards)
- UN/EDIFACT Message Standards (Electronic data interchange specifications)
- UNCTAD Recommendations and Standards for Single Windows
- WTO Trade Facilitation Agreement (TFA) guidelines

1.4 Business Vision

1.4.1 Business Domain

- Unified Trade Ecosystem: Deliver a single platform for import, export, and transit procedures.
- Regulatory Coordination: Strengthen collaboration among agencies to ensure compliance and risk-based decision-making.
- Business Imperative: Reduce transaction costs, accelerate clearance times, and enhance Angola's competitiveness in global trade.

1.4.2 Data Domain

- Data Harmonization: Standardize trade information using the WCO Data Model.
- Interoperability: Enable seamless data exchange across agencies and international partners.
- Business Imperative: Improve transparency, predictability, and trust in trade flows through consistent, reliable information.

1.4.3 Application Domain

- Single Window Portal: Provide a centralized communication and information system aligned with UNCTAD's framework.
- Workflow Automation: Digitize end-to-end trade processes, minimizing manual intervention.
- Business Imperative: Enhance efficiency, reduce delays, and support Angola's obligations under the WTO Trade Facilitation Agreement.

1.4.4 Technology Domain

- Scalable Infrastructure: Deploy modular, cloud-native architecture to support growth and resilience.
- Security & Trust: Implement strong cybersecurity and identity management to protect sensitive trade data.
- Business Imperative: Ensure system reliability, resilience, and stakeholder confidence in digital trade operations.

1.4.5 Supply Chain Domain

- Event Logging & Traceability: Monitor land and maritime supply chains with integrated tracking.
- Visibility & Accountability: Provide end-to-end transparency across logistics operations.
- Business Imperative: Strengthen resilience, reduce risks, and build trust among traders, regulators, and international partners.

2 Enterprise Architecture

The JUL system implementation follows a phased approach to managing complexity and ensuring business value delivery at each stage:

2.1 Project Phasing

- Core platform setup, including IAM, company management, and basic declaration processing with ASYCUDA integration. Phase 1 (Foundation):

- SINTECE integration, license management, agent nomination, and document management capabilities. Phase 2 (Integration):
- Advanced workflow automation, OGA integrations, comprehensive reporting, and analytics capabilities. Phase 3 (Enhancement):
- Performance optimization, advanced security features, mobile applications(Optional), and AI-powered risk management(Optional). Phase 4 (Optimization):

Tool Category	License Type	Tool Category	License Type
UML Modeling Enterprise Architect / PlantUML	Open Source / Commercial	Configuration Git / GitLab	Open Source
IDE Visual Studio 2022 / VS Code	Commercial / Open Source	Syntax Check SonarQube	Commercial
HTML/CSS/JS ESLint / Prettier / StyleLint	Open Source	Data/SQL Check pgAdmin / DBeaver	Open Source
Integration Architect Postman / Swagger	Commercial / Open Source	Web Check Lighthouse / Webpage Test	Open Source
Unit Test xUnit / Jest / Jasmine	Open Source	Deployment Kubernetes / Helm / Argo CD	Open Source
Performance Test JMeter / k6	Open Source	Load Test Apache JMeter / Gatling	Open Source
Security Test Checkmarx / OWASP ZAP	Commercial / Open Source	API Test Postman / Rest Assured	Commercial / Open Source
Container Docker / Harbor	Open Source	Monitoring Prometheus / Grafana	Open Source
Log Management ELK Stack (Elasticsearch)	Open Source / Commercial	Code Quality SonarQube / SonarLint	Commercial / Open Source
Version Control GitLab / GitHub	Commercial / Open Source	CI/CD GitLab CI / Jenkins	Open Source
Database PostgreSQL / pgAdmin	Open Source	Trace/Debug Jaeger / OpenTelemetry	Open Source
Package Manager npm / NuGet	Open Source	Documentation Swagger UI / ReDoc	Open Source

2.2 Technology and Architecture Assumptions and Dependencies

Assumption & Dependencies	Architecture Decision
Infrastructure Availability: On-premises Kubernetes cluster with adequate compute, storage, and network resources is provisioned and operational.	Deploy on Kubernetes with 3 environments (Dev: 3 nodes, Staging: 5 nodes, Production: 10+ nodes). Each environment is isolated via namespaces with dedicated resource quotas.
External System Connectivity: Network connectivity to ASYCUDA (AGT), SINTECE, and OGA systems is established with appropriate firewall rules and VPN access.	Implement DMZ zone for external integration with the API Gateway. Use certificate-based mutual authentication for ASYCUDA SOAP/XML. REST/JSON for SINTECE and OGAs with OAuth 2.0 token-based authentication.
Database Platform: PostgreSQL database platform is available with high availability configuration and backup infrastructure.	Adopt a database-per-microservice pattern using PostgreSQL 15+. Production: Primary + 2 read replicas per service. Implement streaming replication with automatic failover using Patroni.
Identity Management: An Enterprise identity provider is available for user authentication and authorization integration.	Deploy Keycloak 23+ as a centralized IAM solution. Implement OAuth 2.0/OpenID Connect for API authentication, SAML 2.0 for enterprise SSO. Mandatory MFA for customs officers using TOTP.
Master Data Sources: Nightly batch feeds available from AGT for HS codes, tariff schedules, port codes, and regulatory reference data.	Implement Master Data Management Service with scheduled batch synchronization at 02:00 AM WAT. Use ETL pipeline with data validation, transformation, and distribution to all microservices. Implement rollback capability for failed synchronizations.
Object Storage: A Scalable object storage solution is available for document management with an S3-compatible API.	Deploy MinIO in distributed mode (6+ nodes in production) for S3-compatible object storage. Implement erasure coding for data protection. Integrate with Keycloak for authentication and RBAC.
Message Queue Platform: A Message broker infrastructure is available for asynchronous communication between microservices.	Deploy RabbitMQ 3.12+ in cluster mode (3 nodes) with mirrored queues. Implement dead letter queues for failed messages. Use AMQP protocol with persistent messages for critical events.
Monitoring Infrastructure: Monitoring and logging infrastructure is available for production observability.	Implement Prometheus + Grafana for metrics and visualization. Deploy ELK Stack for centralized logging. Integrate Jaeger for distributed tracing. Configure alerting via email/SMS for critical events.
CI/CD Platform: Source control and CI/CD pipeline infrastructure is available for automated build and deployment.	Use GitLab for source control with GitLab CI for automated pipelines. Implement ArgoCD for GitOps-based Kubernetes deployments. Integrate SonarQube for code quality gates and Checkmarx for security scanning.
Backup Infrastructure: Backup storage and disaster recovery infrastructure are available with off-site replication.	Implement automated backup strategy: Transaction logs every 15 minutes, database backups every 6 hours, full system

Assumption & Dependencies	Architecture Decision
	backup daily. Maintain 30-day retention with a 7-year archive. Cross-site replication to the DR site.
WCO Data Model Documentation: Access to WCO Data Model Version 3.10 specifications and UN/EDIFACT message standards.	Implement a data model fully compliant with WCO Data Model 3.10. Use JSON schemas for API validation. Map database entities to WCO classes (Declaration, Goods Item, Party, etc.). Document deviations from standard.
Data Retention Policy: Legal requirements for data retention (7 years minimum) are documented and approved.	Implement an automated archival process for data older than 1 year to cold storage. Maintain audit trail for 7 years minimum. Implement data lifecycle management with automated deletion after retention period (with legal hold capability).
Business Continuity Plan: Disaster recovery site and procedures are defined with RTO < 4 hours and RPO < 1 hour.	Implement hot standby at the DR site with real-time replication. Maintain a complete environment replica at the DR location. Conduct quarterly DR testing. Document failover and failback procedures. Monitor replication lag continuously.
User Acceptance Testing Environment: A Staging environment with production-like data is available for UAT activities.	Provision a staging environment with 5 Kubernetes nodes (16 vCPU, 64 GB RAM each). Implement data masking for production data copied to staging. Provide dedicated testing slots for business users. Reset the environment weekly.

3 Architecture Objectives

The architecture is designed to achieve the following core objectives:

- Scalability: Support up to 10,000 concurrent users and 100 transactions per second with horizontal scaling capabilities.
- Availability: Achieve 99.9% uptime through redundancy, failover mechanisms, and comprehensive monitoring.
- Performance: Deliver response times under 3 seconds for 95% of API requests through optimized architecture and caching.
- Security: Implement comprehensive security measures, including encryption, authentication, authorization, and audit logging.
- Maintainability: Enable independent deployment and updates of microservices with minimal system disruption.
- Interoperability: Ensure seamless integration with external systems using industry-standard protocols and data formats.
- Compliance: Adhere to WCO Data Model, UN/EDIFACT standards, and Angola regulatory requirements.
- Resilience: Provide disaster recovery capabilities with RTO < 4 hours and RPO < 1 hour.

4 Architecture Constraints

4.1 Standards

4.1.1 Technology Standards

- Frontend: Angular 20+ with TypeScript and Module Federation
- Backend: ASP.NET Core 10.0 with C# for all microservices
- •Database: PostgreSQL 15+ for relational data storage
- •Object Storage: MinIO for S3-compatible document storage
- Authentication: Keycloak 23+ with OAuth 2.0/OpenID Connect/SAML 2.0
- Containerization: Docker with OCI container specifications
- Orchestration: Kubernetes for deployment and scaling

4.1.2 Messaging Standards

- Internal Messaging: RabbitMQ 3.12+ with AMQP protocol
- REST APIs: OpenAPI 3.0 specifications with JSON payloads
- SOAP Integration: SOAP 1.1/1.2 for ASYCUDA legacy systems
- Event Messaging: JSON schema validation for all domain events
- API Gateway: Kong for unified API management and security

4.1.3 XML Standards

- UN/EDIFACT: CUSDEC and CUSRES message formats for customs declarations
- WCO Data Model: XML schemas based on WCO Data Model Version 3.10
- SOAP/XML: Standard SOAP envelope structure for ASYCUDA integration
- Schema Validation: XSD validation for all XML message exchanges

4.1.4 Portability

The architecture is designed with portability in mind using containerization and standard APIs:

- All services are containerized using Docker with OCI standards
- Kubernetes deployment enables cloud-agnostic infrastructure
- Database abstraction layer allows migration between PostgreSQL-compatible systems
- MinIO S3-compatible API enables migration to cloud object storage
- Standard protocols (REST, SOAP) ensure external system portability

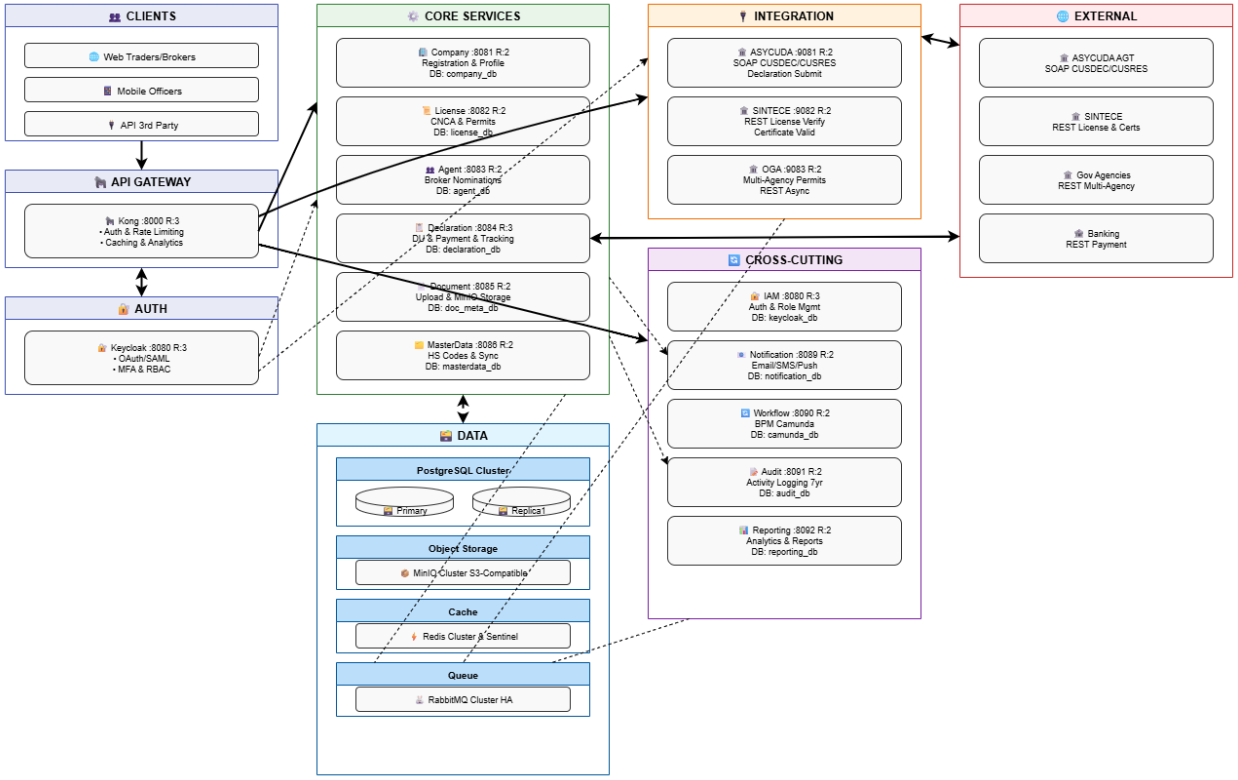
5 Architecture Model

5.1 Component Descriptions

The JUL system employs a microservices architecture consisting of 14+ specialized services grouped into three categories:

- Company Management, License & Permits, Agent Nomination, Declaration Management, Document Management, Master Data Management Core Business Services (6 services):
- ASYCUDA Integration, SINTECE Integration, OGA Integration Services (3 services):

- IAM (Keycloak), Notification, Workflow (Camunda), Audit & Logging, Reporting Cross-Cutting Services (5 services):



5.2 Presentation Layer

The presentation layer provides user interfaces for different stakeholder groups using Angular 20+ with Module Federation for micro-frontend architecture:

- Web Portal: Responsive design supporting desktop and mobile web browsers
- User Roles: Traders, Customs Brokers, Freight Forwarders, Customs Officers, System Administrators
- Localization: Full Portuguese and English language support with dynamic switching
- Accessibility: WCAG 2.1 AA compliant with screen reader support
- Progressive Web App: Offline capabilities for essential functions
- Material Design: Angular Material UI components for a consistent user experience

5.2.1 Key Interface Modules

- Personalized dashboards with role-based information, status updates, and quick actions Dashboard Module
- Registration wizard, profile management, user invitation, document library, Company Management Module
- Step-by-step declaration creation, document attachment, status tracking, payment integration Declaration Module
- Application forms, OGA coordination, renewal processing, compliance tracking, License & Permits Module
- Agent search, power of attorney management, authorization tracking, Agent Nomination Module
- Secure upload, document viewer, collaboration features, advanced search, Document Management Module
- Pre-built templates, custom report builder, data visualization, scheduled delivery, Reporting Module

5.2.2 Business Logic Layer

The business logic layer implements domain-driven design principles with clear bounded contexts:

- Independent services with database-per-service pattern Microservices Architecture
- Event-driven communication for loose coupling between services: Domain Events
- Configurable validation and processing rules, Business Rules Engine
- Camunda 8 for complex business process management, Workflow Orchestration
- Command Query Responsibility Segregation for complex read scenarios, CQRS Pattern

5.2.3 Core Business Services

Company Management Service (Port 8081)

- Company registration and onboarding with verification workflows
- Profile management and updates with document validation
- User-company relationship management
- Integration with Keycloak for user provisioning
- Database: company_db (PostgreSQL)

License & Permits Service (Port 8082)

- CNCA certificate management and processing
- Multi-agency permit coordination
- License renewal and compliance tracking
- Integration with SINTECE for verification
- Database: license_db (PostgreSQL)

Agent Nomination Service (Port 8083)

- Customs broker/agent nomination processing
- Power of attorney management
- Authorization validity monitoring
- Agent performance tracking
- Database: agent_db (PostgreSQL)

Declaration Management Service (Port 8084)

- DU (Declaração Única) creation and validation
- State machine for declaration lifecycle
- Integrated payment processing
- ASYCUDA integration for customs processing
- Workflow management via Camunda
- Database: declaration_db (PostgreSQL)

Document Management Service (Port 8085)

- Secure document upload and storage
- MinIO integration for object storage
- Document validation and format verification

- Metadata management and search
- Database: document_metadata_db + MinIO storage

Master Data Management Service (Port 8086)

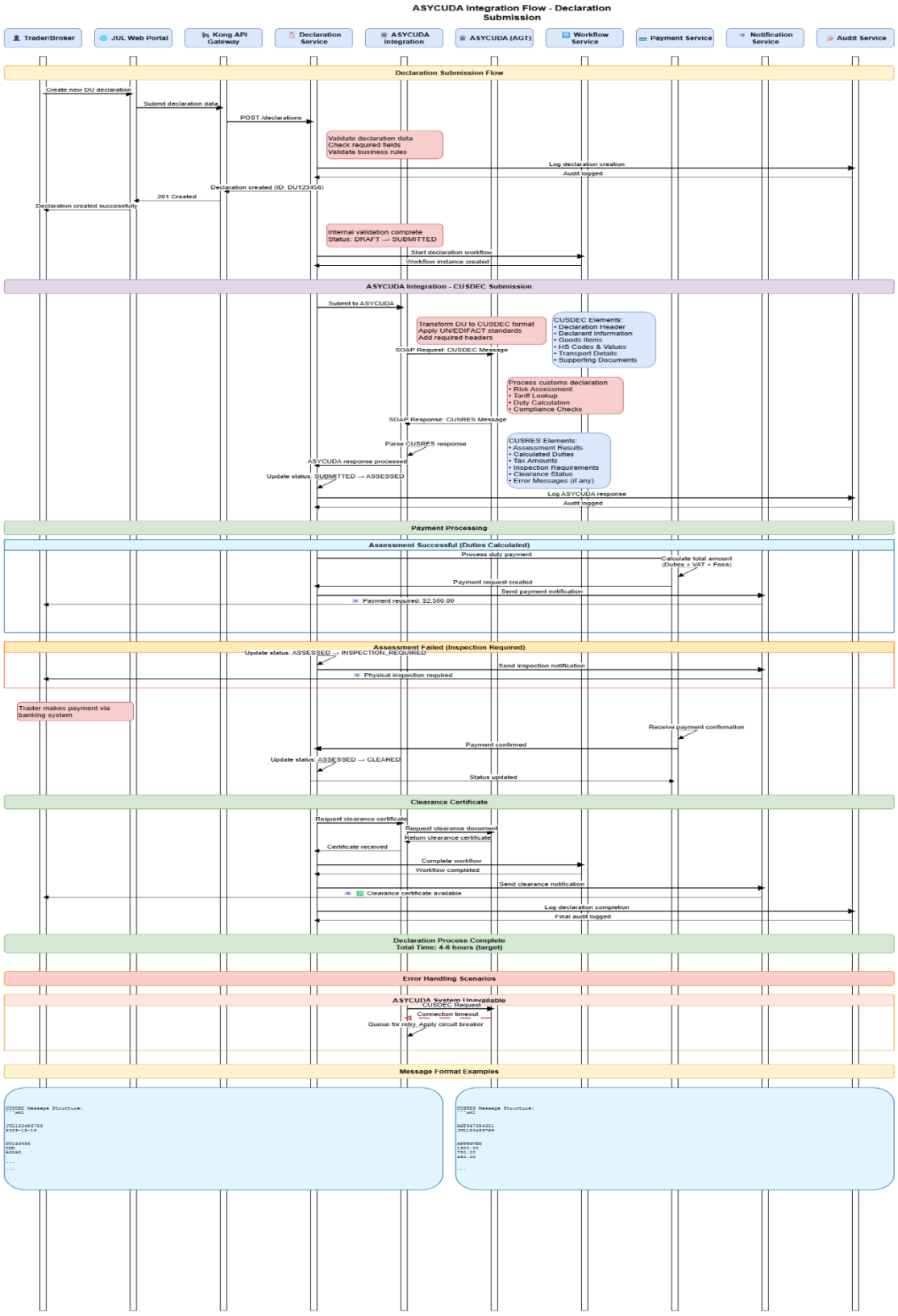
- Nightly batch synchronization from AGT systems
- HS Code management (WCO HS2017/2022)
- Port codes, country codes, currency codes
- Distribution to all microservices
- Database: masterdata_db (PostgreSQL)

5.3 Services and Integration Layer

5.3.1 Integration Services

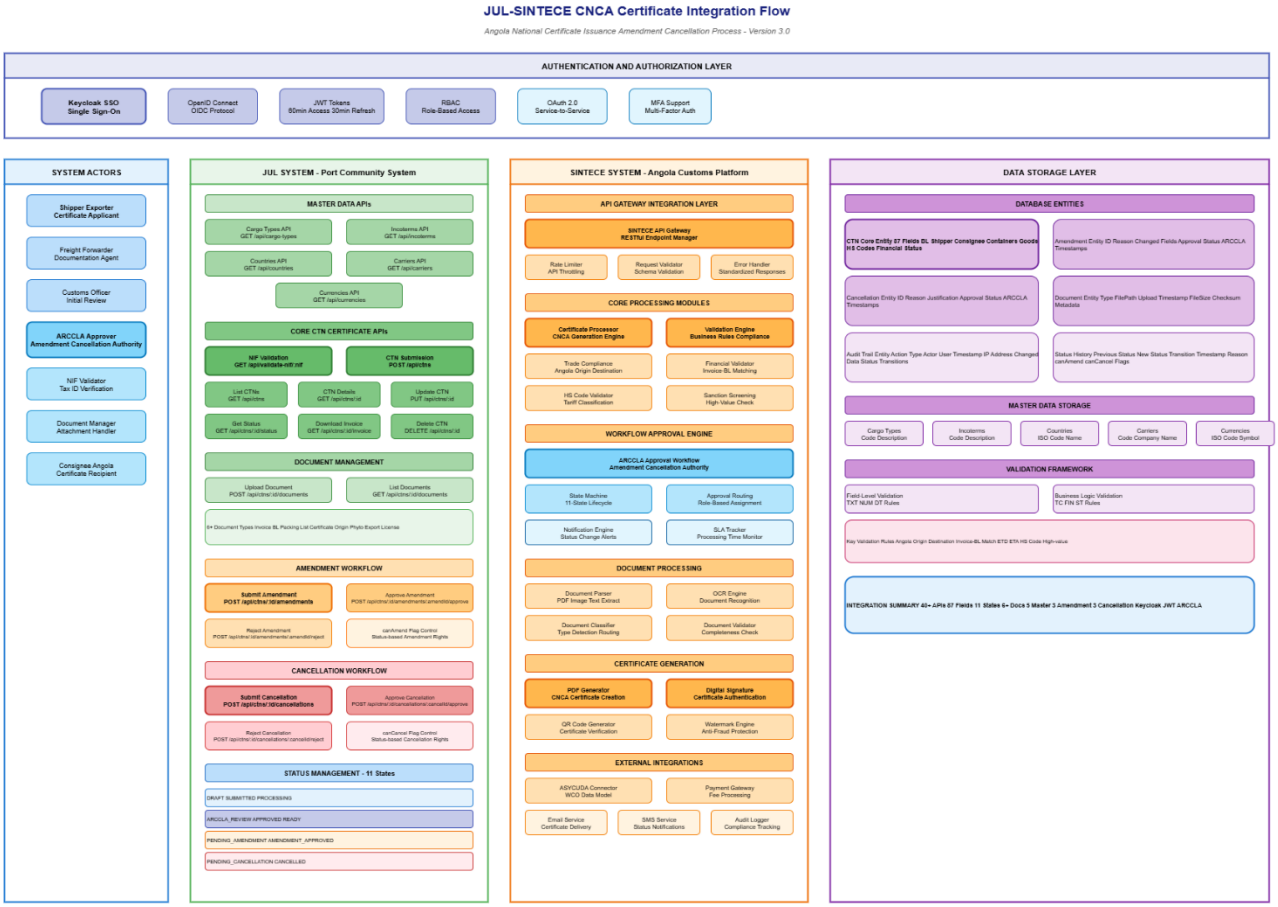
ASYCUDA Integration Service (Port 9081)

- SOAP/XML message handling for customs declarations
- CUSDEC submission and CUSRES response processing
- Duty calculation and assessment results
- Clearance certificate retrieval


ASYCUDA Integration Flow - Declaration Submission
Trader/Broker
JUL Web Portal
Kong API Gateway
Declaration Service
ASYCUDA Integration
ASYCUDA (AGT)
Workflow Service
Payment Service
Notification Service
Audit Service
Declaration Submission Flow
Create new DU declaration
Submit declaration data
POST /declarations
Validate declaration data
Check required fields
Validate business rules
Log declaration creation
Audit logged
Declaration created (ID: DU123456)
201 Created
Declaration created successfully
Internal validation complete
Status: DRAFT → SUBMITTED
Start declaration workflow
Workflow instance created
ASYCUDA Integration - CUSDEC Submission
Submit to ASYCUDA
Transform DU to CUSDEC format
Apply UN/EDIFACT standards
Add required headers
CUSDEC Elements:
• Declaration Header
• Declarant information
• Goods Items
• HS Codes & Values
• Transport Details
• Supporting Documents
SOAP Request: CUSDEC Message
Process customs declaration
• Risk Assessment
• Tariff Lookup
• Duty Calculation
• Compliance Checks
SOAP Response: CUSRES Message
Parse CUSRES response
CUSRES Elements:
• Assessment Results
• Calculated Duties
• Tax Amounts
• Inspection Requirements
• Clearance Status
• Error Messages (if any)
ASYCUDA response processed
Update status: SUBMITTED → ASSESSED
Log ASYCUDA response
Audit logged
Payment Processing
Assessment Successful (Duties Calculated)
Process duty payment
Calculate total amount
(Duties + VAT + Fees)
Payment request created
Send payment notification
Payment required: $2,500.00
Assessment Failed (Inspection Required)
Update status: ASSESSED → INSPECTION_REQUIRED
Send inspection notification
Physical inspection required
Trader makes payment via banking system
Receive payment confirmation
Payment confirmed
Update status: ASSESSED → CLEARED
Status updated
Clearance Certificate
Request clearance certificate
Request clearance document
Return clearance certificate
Certificate received
Complete workflow
Workflow completed
Send clearance notification
Clearance certificate available
Log declaration completion
Final audit logged
Declaration Process Complete
Total Time: 4-6 hours (target)
Error Handling Scenarios
ASYCUDA System Unavailable
CUSDEC Request
Connection timeout
Queue for retry, Apply circuit breaker
Message Format Examples
CUSDEC Message Structure:
CUSRES Message Structure:

SINTECE Integration Service (Port 9082)

- REST/JSON API integration
- License and permit verification
- Certificate validation and authenticity checking
- Single window data synchronization



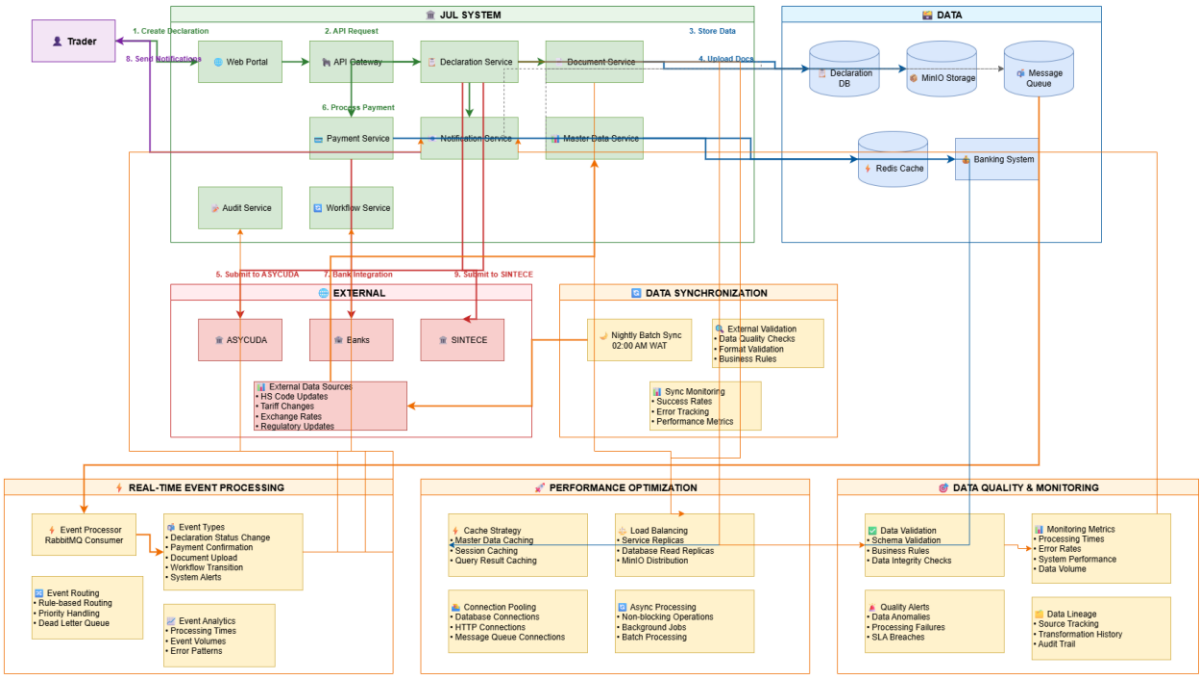
OGA Integration Service (Port 9083)

- Multi-agency REST/JSON integration
- LPCO requirements coordination
- Regulatory certificate management
- Asynchronous processing via message queue

5.3.2 Data Flow

Data flows through the system following these patterns

- User submits declaration → Declaration Service validates → ASYCUDA Integration sends CUSDEC → Response processed → User notified Synchronous Flow
- License application → Queue message → OGA Integration → External processing → Status update event → User notification Asynchronous Flow
- Declaration state change → Event published → Multiple services react → Audit logged → Reports updated Event-Driven Flow



5.4 Data Access Layer

5.4.1 Data Access Control

Data access is controlled through multiple security layers:

- Row-Level Security: PostgreSQL RLS policies enforce tenant isolation
- Column-Level Encryption: Sensitive fields encrypted at the application layer
- API-Level Authorization: OAuth 2.0 scopes and role-based permissions
- Audit Logging: Complete tracking of data access and modifications

5.4.2 Data Storage

Storage Type	Technology	Use Case
Relational Database	PostgreSQL 15+	Transactional data, master data, user data
Object Storage	MinIO	Documents, attachments, large files
Cache	Redis 7+	Session data, frequently accessed data
Message Queue	RabbitMQ 3.12+	Asynchronous messaging, event processing

5.4.3 Connection Pooling

Connection pooling optimizes database performance:

- Connection Pool Size: Min 10, Max 100 connections per service
- Connection Lifetime: Maximum 30 minutes with automatic renewal

- Connection Validation: Health checks before query execution
- Connection Timeout: 30 seconds for acquiring a connection from the pool

5.4.4 Concurrent Access and Object Locking

Concurrency is managed through multiple mechanisms:

- Optimistic Locking: Version numbers on critical entities
- Pessimistic Locking: Database row locks for financial transactions
- Distributed Locks: Redis-based locks for cross-service operations
- Idempotency Keys: Prevent duplicate transaction processing

5.4.5 Transactional Requirements

ACID properties are maintained through:

- Local Transactions: PostgreSQL ACID guarantees within service boundaries
- Distributed Transactions: Saga pattern for cross-service operations
- Compensation Logic: Automated rollback for failed distributed transactions
- Transaction Isolation: Read Committed isolation level for most operations

5.4.6 Persistence

Data persistence strategy ensures durability:

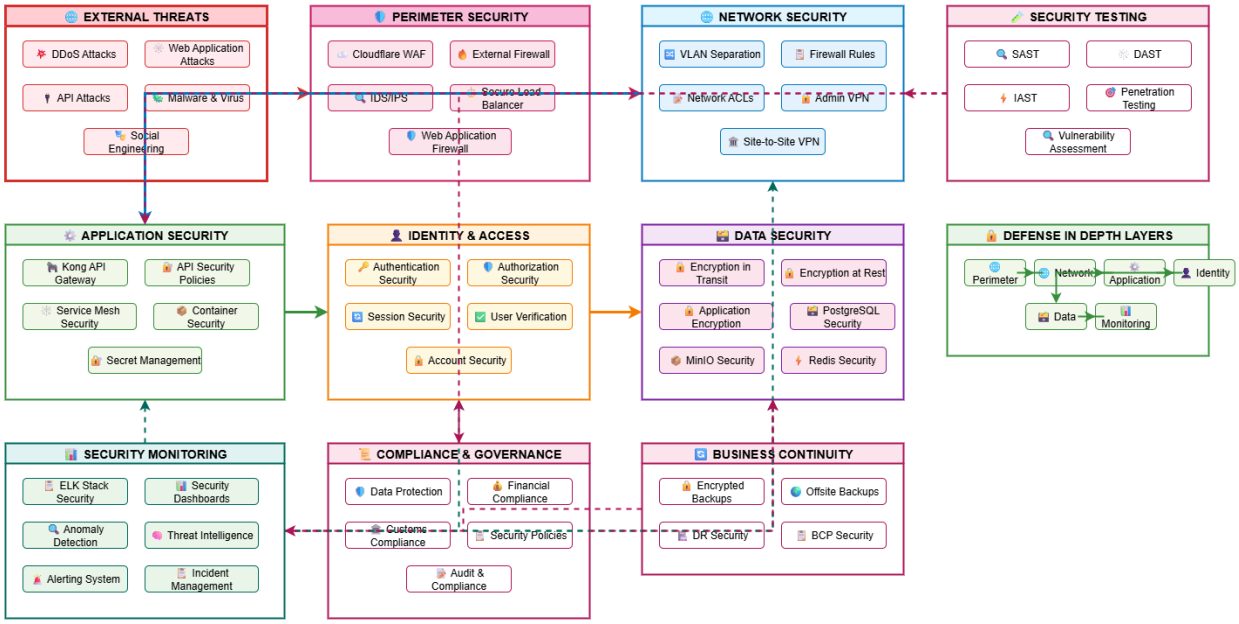
- Write-Ahead Logging: PostgreSQL WAL for crash recovery
- Replication: Streaming replication to read replicas
- Point-in-Time Recovery: Continuous archiving of WAL files
- Backup Strategy: Full daily backups plus continuous WAL archiving

5.5 Performance

Performance targets and optimization strategies:

Metric	Target	Strategy
API Response Time	< 3 seconds (95%ile)	Caching, database indexing, CDN
Throughput	100 TPS	Horizontal scaling, load balancing
Concurrent Users	10,000	Stateless services, session clustering
Database Query	< 500ms (95%ile)	Query optimization, materialized views
Page Load Time	< 2 seconds	Code splitting, lazy loading, and compression

5.7 Security



5.7.1 Authentication

5.7.2 Authentication

- Identity Provider: Keycloak 23+ with OAuth 2.0/OpenID Connect
- Multi-Factor Authentication: TOTP/SMS required for customs officers
- Password Policy: Minimum 12 characters, complexity requirements, 90-day rotation
- Session Management: JWT tokens with 30-minute expiry, refresh tokens for 7 days
- Single Sign-On: SAML 2.0 for enterprise integration

5.7.3 Authorization

- Role-Based Access Control: Fine-grained permissions per role
- Resource-Level Permissions: User can only access their own company data
- API Scopes: OAuth 2.0 scopes limit API access
- Dynamic Authorization: Permissions evaluated at runtime based on context

5.7.4 Access Request Process

User access is granted through a formal workflow:

- Step 1: User submits access request through the portal
- Step 2: The Company administrator reviews and approves
- Step 3: System administrator provisions the user in Keycloak
- Step 4: User receives email with activation link
- Step 5: User sets password and enables MFA if required

- Step 6: Access logged-in audit trail

5.7.5 Encryption

- Data in Transit: TLS 1.3 with modern cipher suites
- Data at Rest: AES-256 encryption for databases and object storage
- Field-Level Encryption: Additional encryption for PII and financial data
- Key Management: Hardware Security Module or software KMS

5.8 Scalability

System scales horizontally across multiple dimensions:

- Stateless Services: All application services are stateless for easy horizontal scaling
- Database Read Replicas: PostgreSQL replicas for read-heavy workloads
- Kubernetes HPA: Automatic pod scaling based on CPU/memory metrics
- Message Queue Clustering: RabbitMQ cluster scales with message volume
- Object Storage: MinIO distributed deployment scales storage capacity
- CDN Integration: Static content delivery scales geographically

5.9 Extensibility

Architecture supports future extensions:

- Plugin Architecture: New services can be added without modifying existing services
- API Versioning: Multiple API versions supported simultaneously
- Event-Driven: New services can subscribe to existing events
- Feature Flags: New features can be gradually rolled out
- Microservices: New capabilities added as independent services

6 Data Conversion and Migration

6.1 Migration Strategy

Initial data migration for Phase 1 deployment follows a phased approach with comprehensive validation and rollback capabilities. Master data is synchronized from authoritative sources (AGT, SINTECE) with automated quality checks. Transactional data remains in source systems initially with on-demand access.

Module	Business Object	Owner	Source Table	Constraints	Target Table	Interface	Rule Sequence
Master Data	HS Codes	AGT Customs	AGT_HS_CODES	Unique HS code (6-10 digits), Valid tariff rate, Active status	hs_codes	Batch ETL	1. Validate format 2. Check WCO compliance 3. Map tariff rates 4. Insert/Update
Master Data	Country Codes	AGT Customs	AGT_COUNTRIES	ISO 3166-1 alpha-2, Valid country name	countries	Batch ETL	1. Validate ISO code 2. Map names 3. Set active flag

Module	Business Object	Owner	Source Table	Constraints	Target Table	Interface	Rule Sequence
Master Data	Currency Codes	AGT Customs	AGT_CURRENCIES	ISO 4217 code, Valid exchange rate	currencies	Batch ETL	1. Validate ISO code 2. Validate rate 3. Set effective date
Master Data	Port Codes	AGT Customs	AGT_PORTS	UN/LOCODE format, Valid port name	ports	Batch ETL	1. Validate LOCODE 2. Verify coordinates 3. Map customs office
Master Data	Customs Offices	AGT Customs	AGT_OFFICES	Unique office code, Valid address	customs offices	Batch ETL	1. Validate code 2. Map region 3. Set operating hours
Company Mgmt	Company Registry	SINTECE	SINTECE_COMPANIES	Valid NIF, Unique registration number, Active status	companies	API Sync	1. Validate NIF format 2. Check duplicates 3. Verify documents 4. Set status
Company Mgmt	Company Documents	SINTECE	SINTECE_DOCS	Valid document type, Not expired	company documents	API Sync	1. Validate type 2. Check expiry 3. Upload to MinIO 4. Link to company
IAM	User Accounts	Manual Import	USER_IMPORT.CSV	Valid email, Unique username, Valid role	keycloak_users	Bulk Import	1. Validate email 2. Check duplicates 3. Generate temp password 4. Send activation
IAM	User Roles	Manual Config	ROLES_CONFIG.CSV	Valid role name, Valid permissions	keycloak_roles	Manual Config	1. Create role 2. Assign permissions 3. Map to groups
License Mgmt	License Types	SINTECE	SINTECE_LICENSE_TYPES	Valid type code, Active status	license types	API Sync	1. Validate code 2. Map requirements 3. Set validity period
License Mgmt	Existing Licenses	SINTECE	SINTECE_LICENSES	Valid license number, Not expired, Valid holder	licenses	API Sync	1. Validate number 2. Check expiry 3. Verify holder 4. Import documents

Module	Business Object	Owner	Source Table	Constraints	Target Table	Interface	Rule Sequence
Master Data	Document Types	AGT Customs	AGT_DOC_TYPES	Unique type code, Valid description	document types	Batch ETL	1. Validate code 2. Map category 3. Set requirements
Master Data	Unit Measures	AGT Customs	AGT_UNITS	UN/CEFACT code, Valid conversion factor	unit measures	Batch ETL	1. Validate UN code 2. Set conversion 3. Map aliases
Master Data	Tariff Schedules	AGT Customs	AGT_TARIFFS	Valid HS code FK, Valid duty rate, Effective dates	tariff schedules	Batch ETL	1. Validate HS code 2. Check dates 3. Validate rates 4. Set preferences
Declaration	Historical Declarations	ASYCUDA	ASYCUDA_DECLARATIONS	Complete declaration, Valid status	Not Migrated	On-Demand API	Access via ASYCUDA API as needed - no bulk migration

6.2 Data Quality Assurance

- Validation Rules: Business rules applied during import to ensure data integrity, format compliance, and referential integrity
- Duplicate Detection: Automated identification of duplicate records based on natural keys (NIF, HS codes, license numbers)
- Data Cleansing: Standardization of formats (dates, phone numbers, addresses), removal of special characters, trimming whitespace
- Reconciliation Reports: Detailed comparison of source vs target data with record counts, field-level differences, and error logs
- Rollback Capability: Point-in-time database snapshots before migration with the ability to revert failed migrations completely
- Error Handling: Failed records logged to the error table with reason codes, reprocessing capability, and notification to data owners
- Data Profiling: Pre-migration analysis of source data quality, completeness, and patterns to identify potential issues
- Staging Environment: All migrations are tested in the staging environment before production with user acceptance testing

7 Reporting and Information

This section describes the strategy for creating reports for each use case that involves reporting capabilities. Reports support operational monitoring, regulatory compliance, and business intelligence requirements.

7.1 Reporting Strategy

The reporting architecture provides three tiers of reporting: (1) Operational reports for day-to-day monitoring, (2) Compliance reports for regulatory requirements, and (3) Business intelligence dashboards for strategic decision-making. All reports support multiple export formats (PDF, Excel, CSV) and can be scheduled for automated delivery

Use Case	Subject Domain	Business Object	Type Report	Description	Comment
UC-001: Monitor Declaration Processing	Operations	Declaration	Operational	Declaration statistics, including volume, processing times, clearance rates by status, customs office, and time period	Real-time dashboard with drill-down capability. Exportable to Excel/PDF
UC-002: Track Payment Transactions	Finance	Payment	Operational	Payment transaction volumes, collection amounts, payment methods, and reconciliation status by date range	Daily reconciliation report with bank statement matching
UC-003: Monitor User Activity	Security	User	Operational	Login statistics, feature usage, session duration, concurrent users, failed login attempts by user role, and time	Security monitoring with alerting on suspicious patterns
UC-004: System Performance Metrics	Operations	System	Operational	API response times, system availability, error rates, throughput by service and endpoint, with percentile breakdown	Technical monitoring dashboard integrated with Prometheus/Grafana
UC-005: Integration Health Status	Operations	Integration	Operational	External system connectivity status, transaction success rates, average response times for ASYCUDA, SINTECE, and OGAs	Real-time status board with alerting on failures
UC-006: Audit Trail Report	Compliance	Audit Log	Compliance	Complete user activity and data modification history with user, timestamp, action, old/new values for the audit period	Required for regulatory audits. 7-year retention. Immutable logs

Use Case	Subject Domain	Business Object	Type Report	Description	Comment
UC-007: WTO TFA Compliance	Compliance	Declaration	Compliance	Trade Facilitation Agreement compliance indicators: average clearance time, document requirements, and advance rulings	Quarterly submission to WTO. Benchmarking against international standards
UC-008: Security Incident Report	Security	Security Event	Compliance	Access logs, authentication failures, authorization violations, and security incidents by severity and user	Security operations center (SOC) report. Incident response tracking
UC-009: Data Retention Compliance	Compliance	All Objects	Compliance	Evidence of compliance with the 7-year data retention requirement showing archived records by object type and date	Annual audit report. Demonstrates legal compliance
UC-010: Trade Statistics Dashboard	Business Intelligence	Declaration	Dashboard	Real-time visualization of import/export volumes, top commodities, trading partners, revenue by HS code, and country	Executive dashboard with charts and graphs. Auto-refresh every 5 minutes
UC-011: Trend Analysis Report	Business Intelligence	Declaration	Analytical	Historical comparison and forecasting of trade volumes, seasonal patterns, and growth trends by commodity and region	Monthly strategic planning report. Predictive analytics
UC-012: Customs Revenue Report	Finance	Payment	Operational	Duty collected, VAT collected, other fees by declaration type, HS chapter, customs office, and time period	Daily, weekly, and monthly aggregations. Budget vs actual comparison
UC-013: License Application Status	Operations	License	Operational	License application pipeline: submitted, under review, approved, rejected by license type, and applicant	Operational tracking for license officers. SLA monitoring
UC-014: Agent	Operations	Agent Nomination	Operational	Customs broker/agent activity: declarations filed, success rate,	Agent ranking and performance

Use Case	Subject Domain	Business Object	Type Report	Description	Comment
Performance Report				average processing time, client satisfaction	monitoring. Quality assurance
UC-015: Document Compliance Report	Compliance	Document	Compliance	Required documents submission rate, missing documents, expired certificates by declaration, and commodity	Quality control report. Identifies non-compliance patterns
UC-016: HS Code Usage Analysis	Business Intelligence	HS Code	Analytical	Most frequently used HS codes, tariff revenue by HS chapter, classification disputes, and reclassification trends	Strategic report for tariff policy decisions
UC-017: User Access Report	Security	User Role	Compliance	User access rights, role assignments, permission changes, and access certification status by user and company	Quarterly access review. Compliance with access control policies
UC-018: System Availability Report	Operations	System	Operational	System uptime/downtime, planned maintenance windows, incident response times, and SLA compliance by month	Monthly operations report. SLA tracking and reporting
UC-019: OGA Coordination Report	Operations	OGA Integration	Operational	OGA permit requests, approval rates, average processing time, bottlenecks by agency, and permit type	Multi-agency coordination report. Process improvement
UC-020: Custom Ad-Hoc Reports	All Domains	Any Object	Ad-Hoc	User-defined custom reports using drag-and-drop report builder with filters, grouping, and calculations	Self-service reporting. Export to PDF, Excel, CSV. Save and schedule

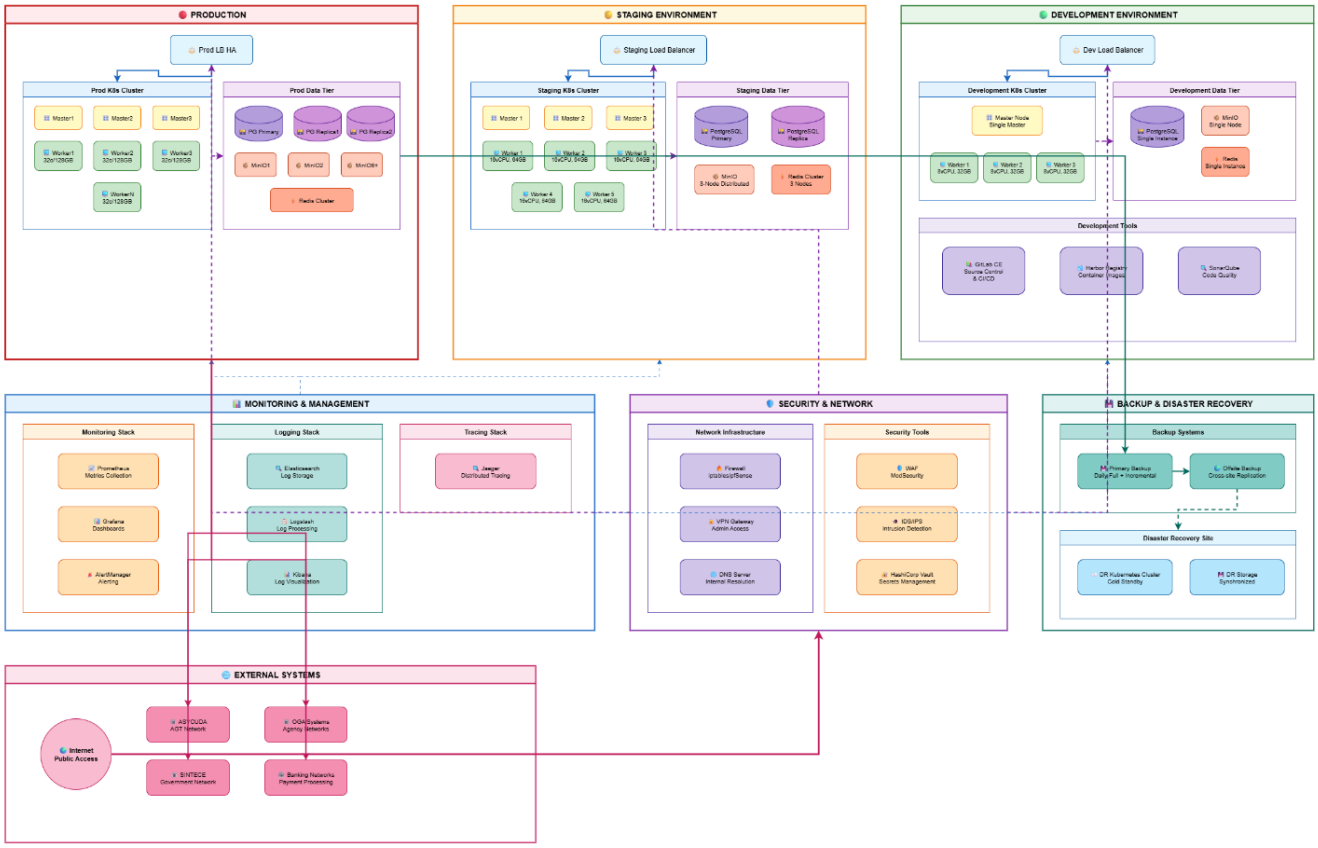
7.2 Report Delivery Options

- Export Formats: PDF (formatted for printing), Excel (with formulas and pivot tables), CSV (for data analysis)
- Scheduled Reports: Daily, weekly, monthly, quarterly schedules with automated email delivery to distribution lists
- On-Demand Generation: Real-time report generation with parameter selection and immediate download
- Dashboard Access: Web-based interactive dashboards with real-time data refresh and drill-down navigation

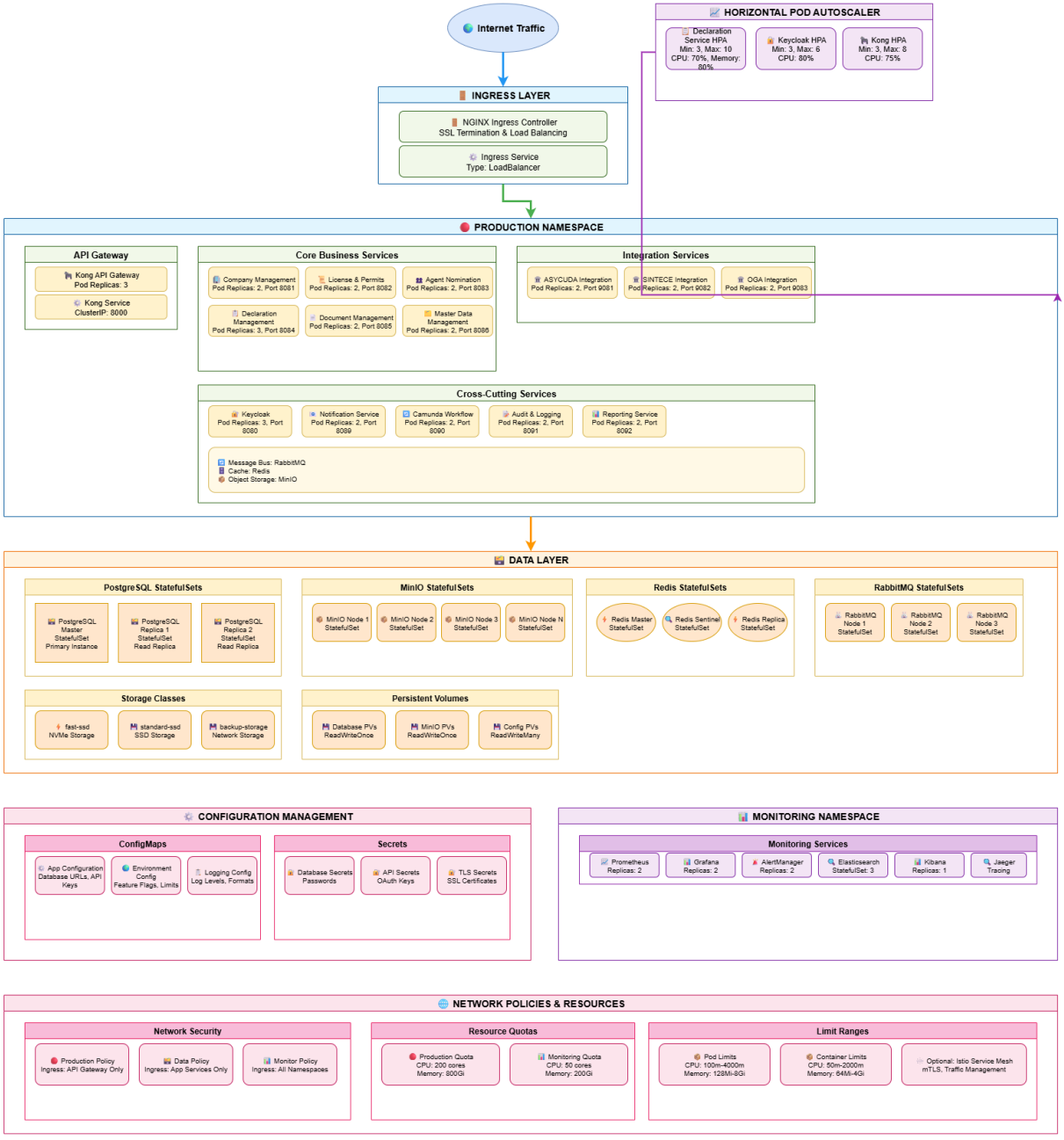
- Mobile Access: Responsive reports optimized for mobile devices with touch-friendly navigation
- API Access: RESTful API endpoints for programmatic report generation and data extraction
- Data Visualization: Charts, graphs, heat maps, and geographical maps for visual data representation
- Report Archival: Automated archival of generated reports for historical reference and compliance

8 Deployment Architecture

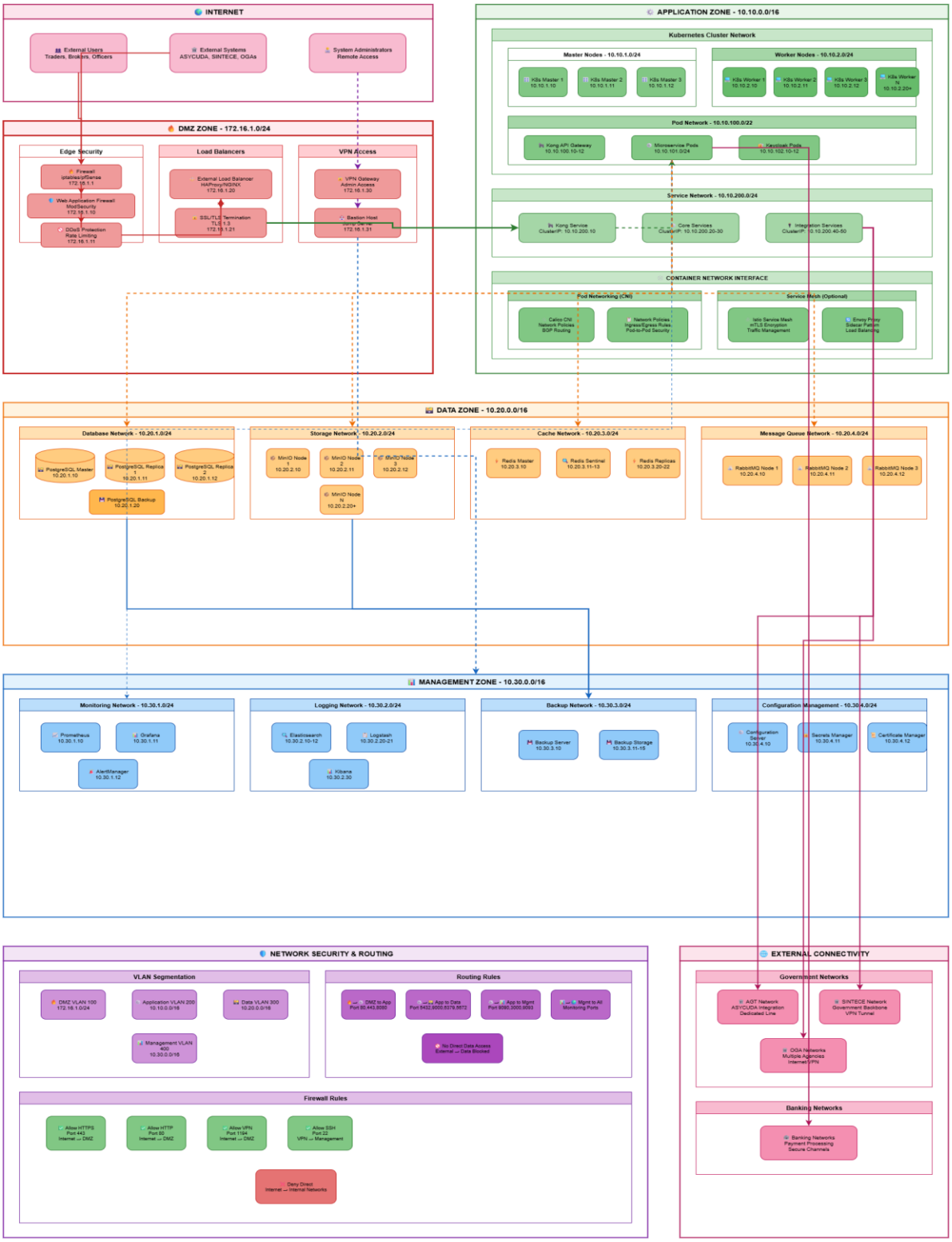
8.1 Deployment Architecture



8.2 Kubernetes Architecture



8.3 Network Architecture



8.4 Environment Specifications

Environment	Nodes	vCPU per Node	RAM per Node	Storage
Production	10+	32	128 GB	20+ TB
Staging	5	16	64 GB	5 TB
Development	3	8	32 GB	2 TB

8.4.1 Kubernetes Configuration

- Control Plane: 3 master nodes for high availability
- Worker Nodes: Distributed across availability zones
- Ingress Controller: NGINX with SSL termination
- Service Mesh: Optional Istio for advanced traffic management
- Storage Classes: Dynamic provisioning for persistent volumes
- Namespaces: Logical separation by environment and function

8.4.2 Network Zones

- DMZ Zone (172.16.1.0/24): Load balancer, WAF, firewall
- Application Zone (10.10.0.0/16): Kubernetes cluster, all services
- Data Zone (10.20.0.0/16): Databases, MinIO, Redis, RabbitMQ
- Management Zone (10.30.0.0/16): Bastion host, monitoring, backups

9 Infrastructure Architecture

9.1 Backup, Failover, and Recovery

9.1.1 Backup

- Transaction Logs: Every 15 minutes to prevent data loss
- Database Backups: Every 6 hours with compression
- Full System Backups: Daily complete backup of all data
- Backup Retention: 30 days active, 7 years archive
- Offsite Storage: Replicated to the disaster recovery site
- Backup Validation: Monthly restore testing

9.1.2 Fail-over

- Database Failover: Automatic promotion of read replica to primary
- Service Failover: Kubernetes restarts failed pods automatically
- Load Balancer Failover: Health checks remove unhealthy backends
- Redis Failover: Sentinel monitors and promotes a new master
- RabbitMQ Failover: Cluster continues with remaining nodes
- Failover Testing: Quarterly chaos engineering exercises

9.1.3 Recovery

- Recovery Time Objective (RTO): < 4 hours for the complete system
- Recovery Point Objective (RPO): < 1 hour maximum data loss
- Database Recovery: Point-in-time recovery from WAL files
- Service Recovery: Kubernetes self-healing restarts services
- Disaster Recovery Site: Full environment at alternate location
- Recovery Procedures: Documented runbooks for all scenarios

9.2 Maintenance Windows

Planned maintenance is scheduled to minimize business impact:

- Regular Maintenance: Sunday 02:00-06:00 WAT (weekly)
- Emergency Maintenance: As needed with advance notification
- Rolling Updates: Zero-downtime deployments for services
- Database Maintenance: During regular window with minimal impact
- User Notification: Email and portal announcements 48 hours in advance
- Maintenance Tracking: All activities logged in the change management system

10 Technology Stack Details

10.1 Microservices Technology Stack

Component	Technology	Version
Frontend Framework	Angular	17+
Backend Framework	ASP.NET Core	8.0
Database	PostgreSQL	15+
Object Storage	MinIO	Latest
Message Queue	RabbitMQ	3.12+
Cache	Redis	7+
IAM	Keycloak	23+
Workflow Engine	Camunda	8

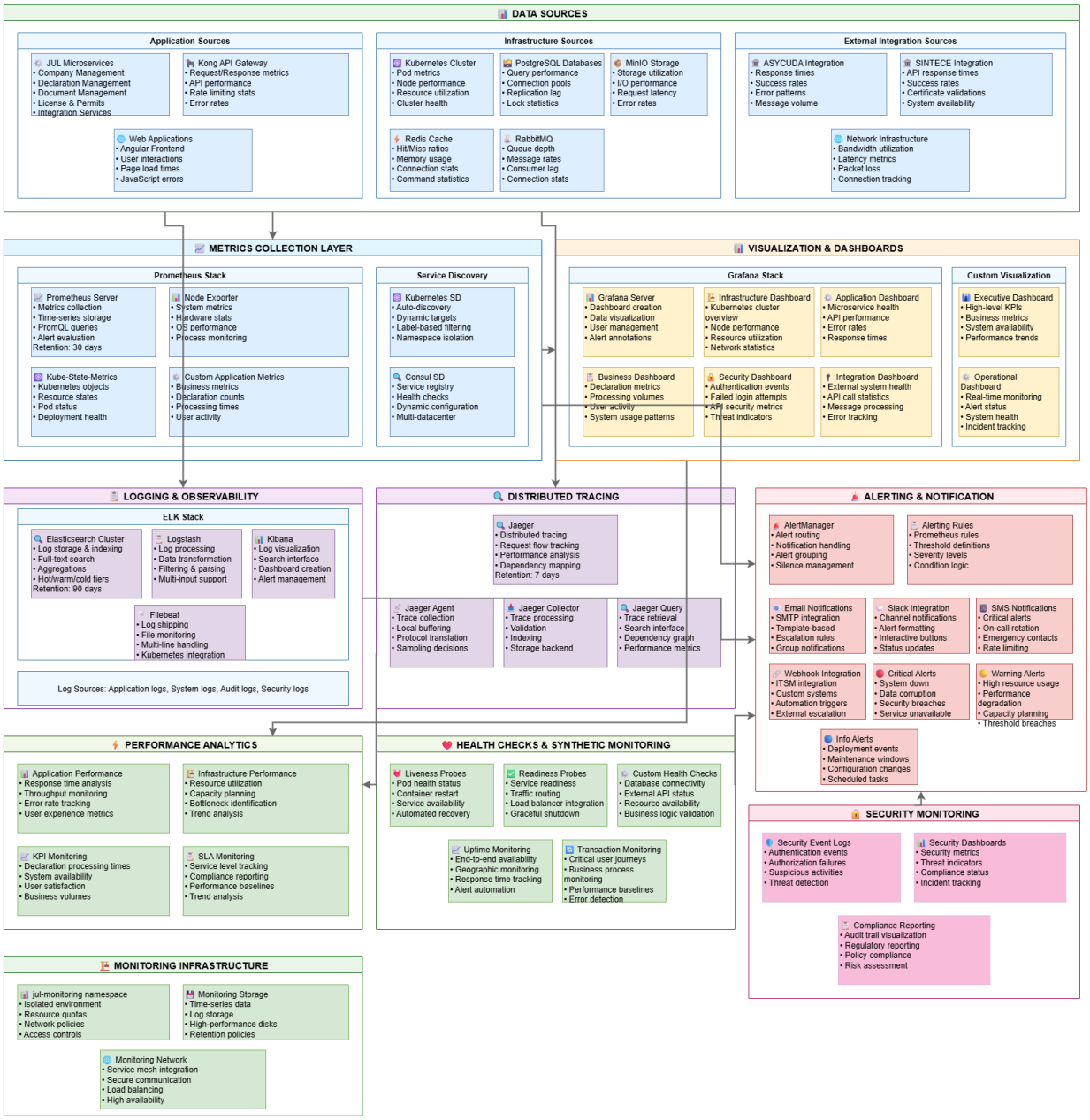
10.2 Integration Protocols

External System	Protocol	Format	Pattern
ASYCUDA (AGT)	SOAP/XML	UN/EDIFACT	Synchronous
SINTECE	REST/JSON	JSON	Synchronous
OGAs	REST/JSON	JSON	Asynchronous
Internal Services	REST/JSON	JSON	Both

10.3 Monitoring and Observability

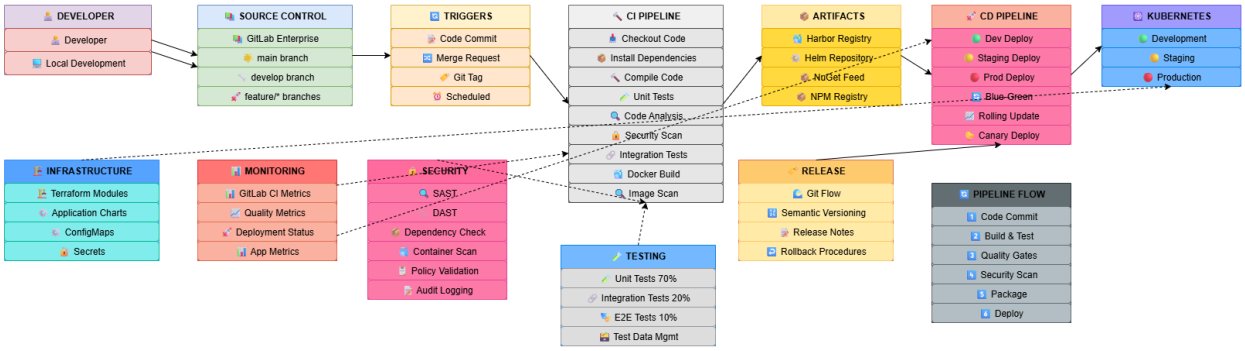
- Metrics Collection: Prometheus scrapes metrics from all services

- Visualization: Grafana dashboards for system and business metrics
- Log Aggregation: ELK Stack (Elasticsearch, Logstash, Kibana) for centralized logging
- Distributed Tracing: Jaeger for request flow tracking across services
- Alerting: Prometheus Alert Manager with email/SMS notifications
- APM: Application Performance Monitoring for user experience tracking
- Health Checks: Kubernetes' liveness and readiness probes



10.4 CI/CD Pipeline

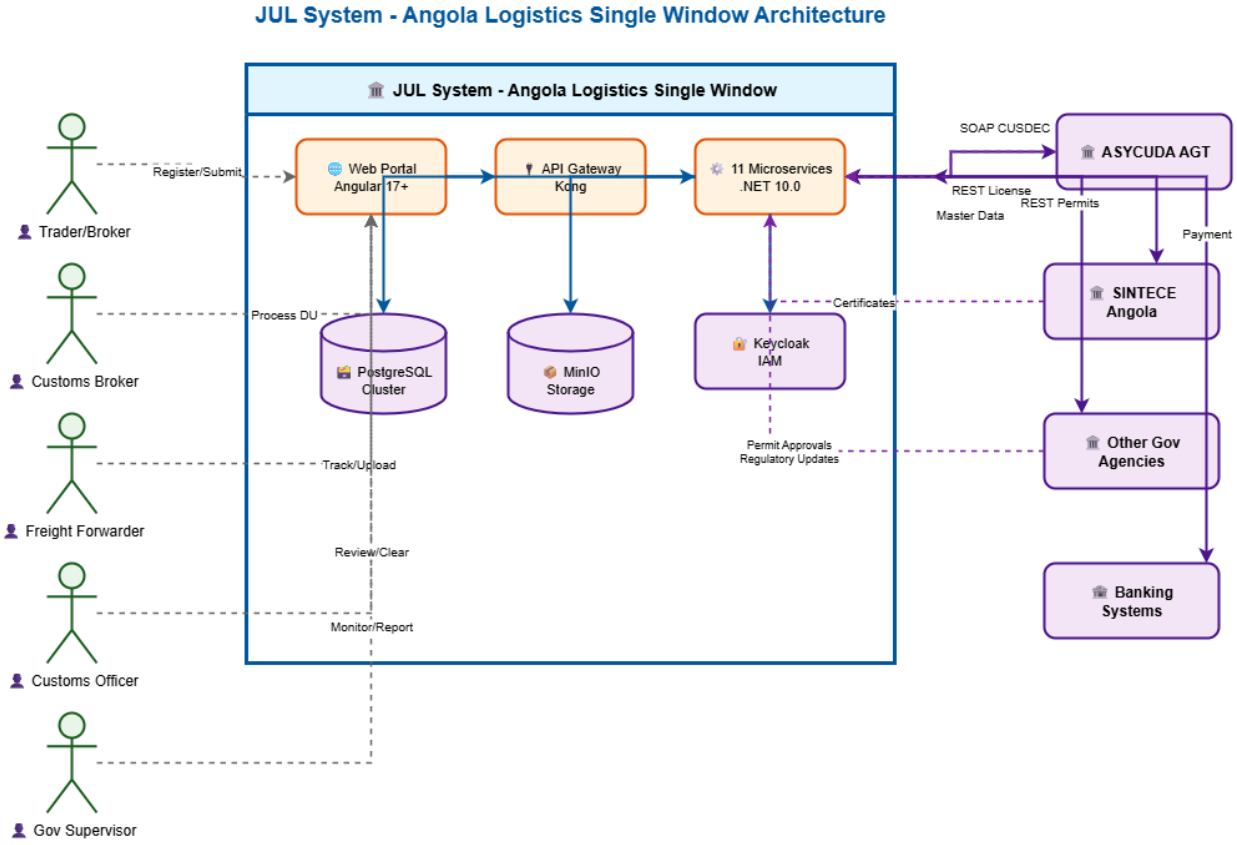
- Source Control: GitLab for version control and collaboration
- CI Pipeline: Automated build, test, and quality gates
- Code Quality: SonarQube for static code analysis
- Security Scanning: Checkmarx for vulnerability detection
- Container Registry: Harbor for private image storage
- CD Pipeline: GitOps-based deployment with ArgoCD
- Environment Promotion: Dev → Staging → Production with approvals



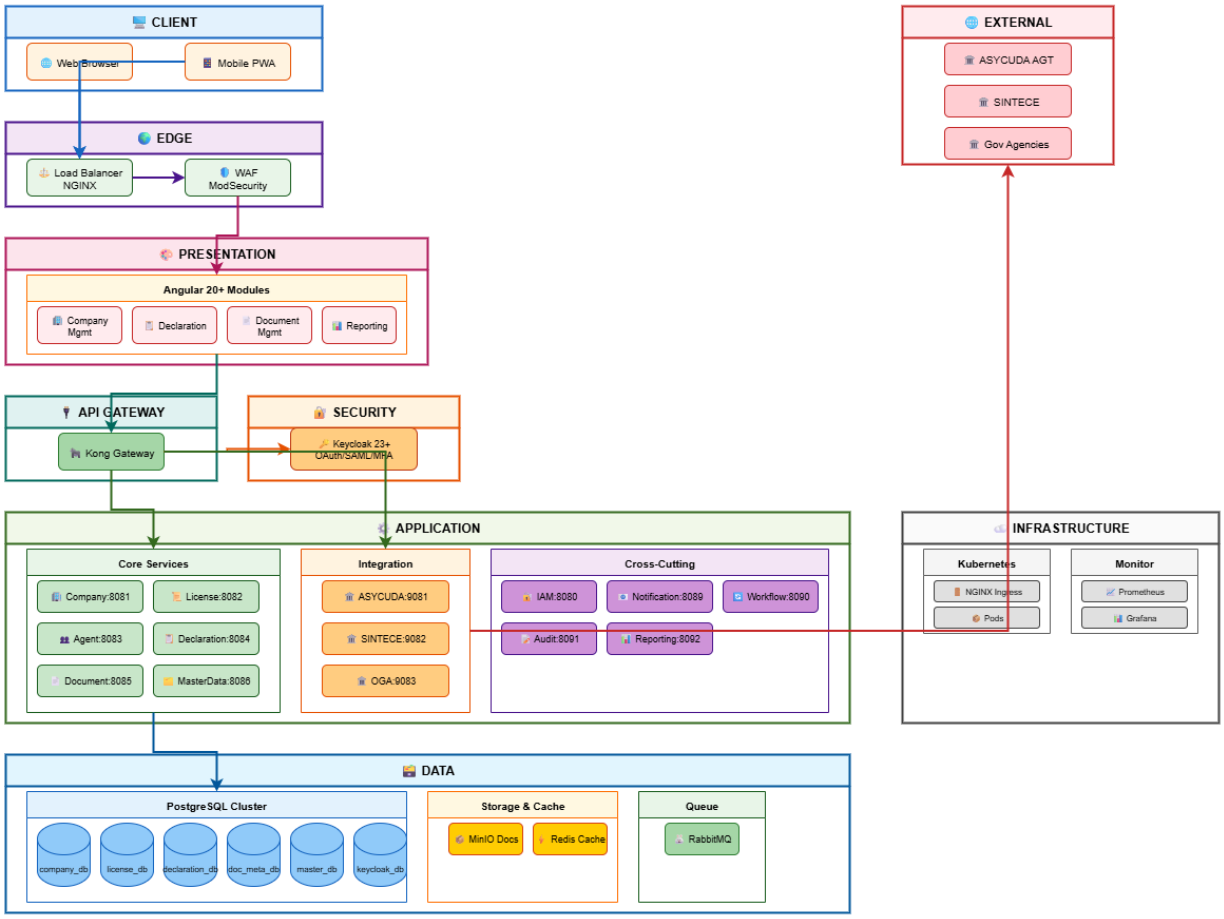
11 Appendices

11.1 Appendix A: Diagram References

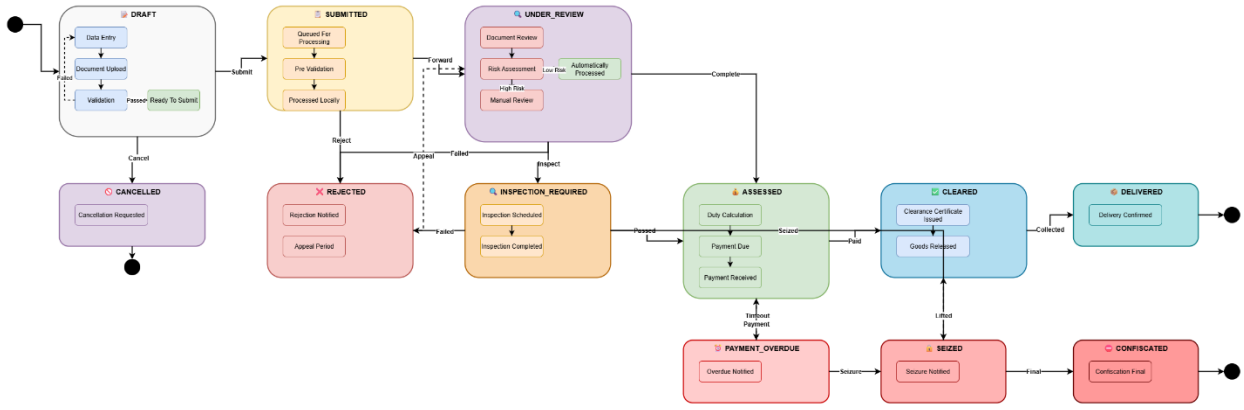
11.1.1 System context and stakeholders



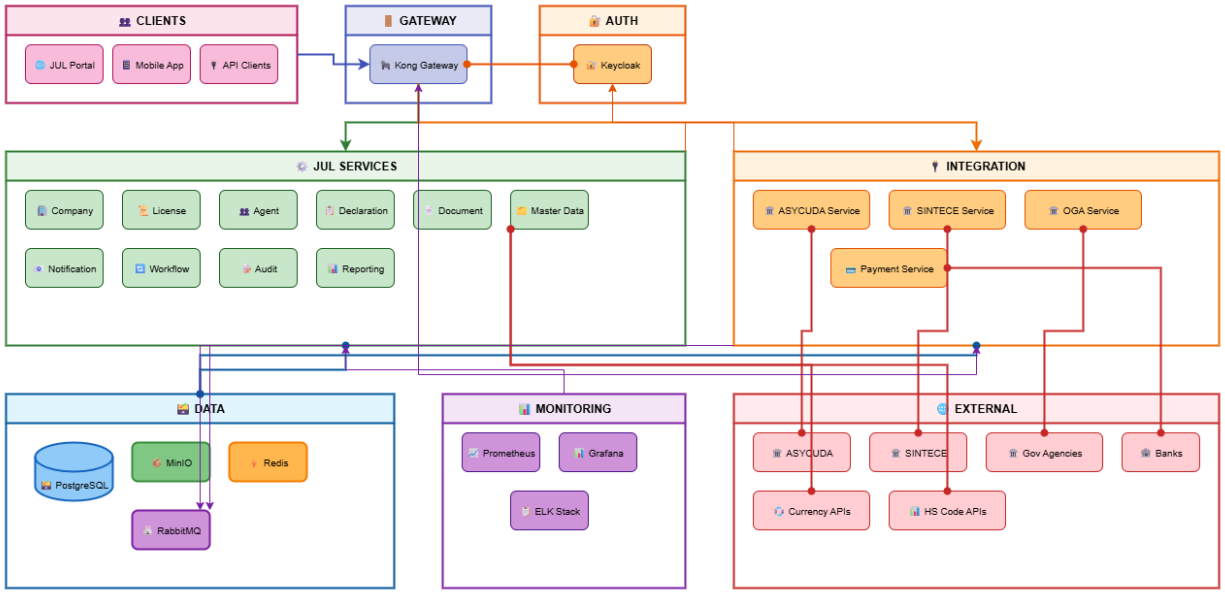
11.1.2 Overall system architecture



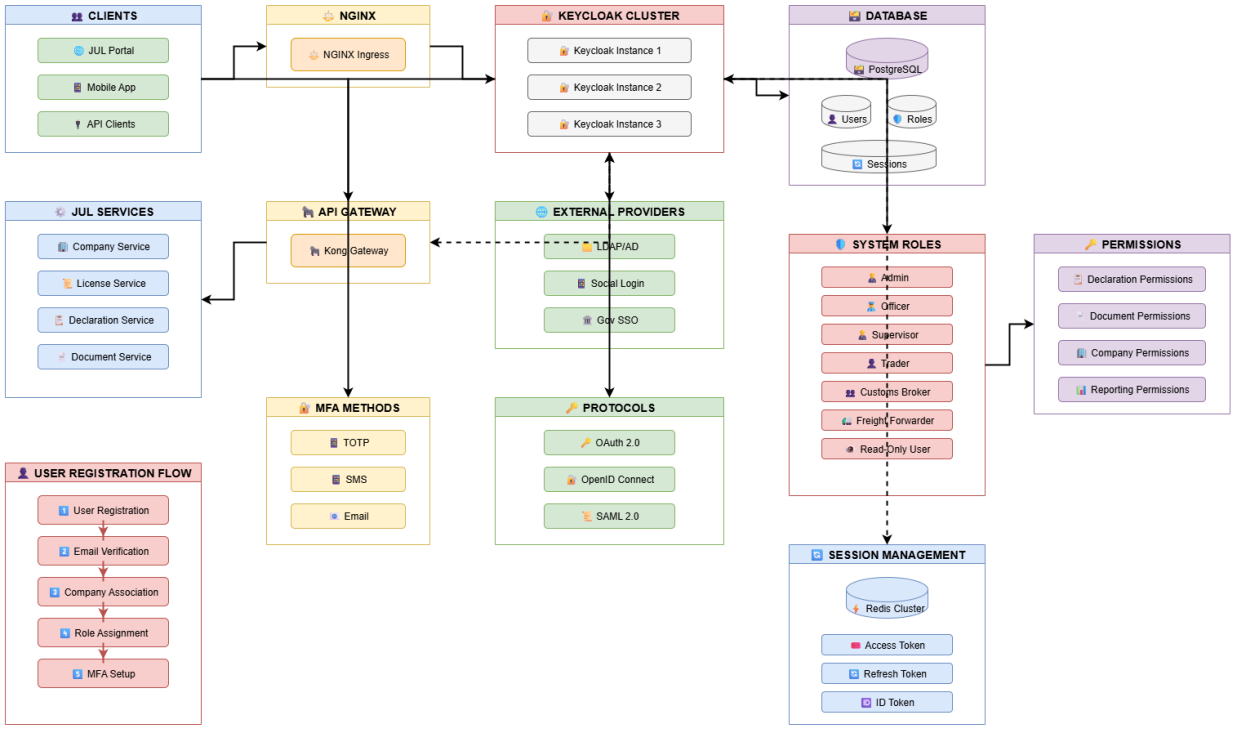
11.1.3 Declaration workflow states



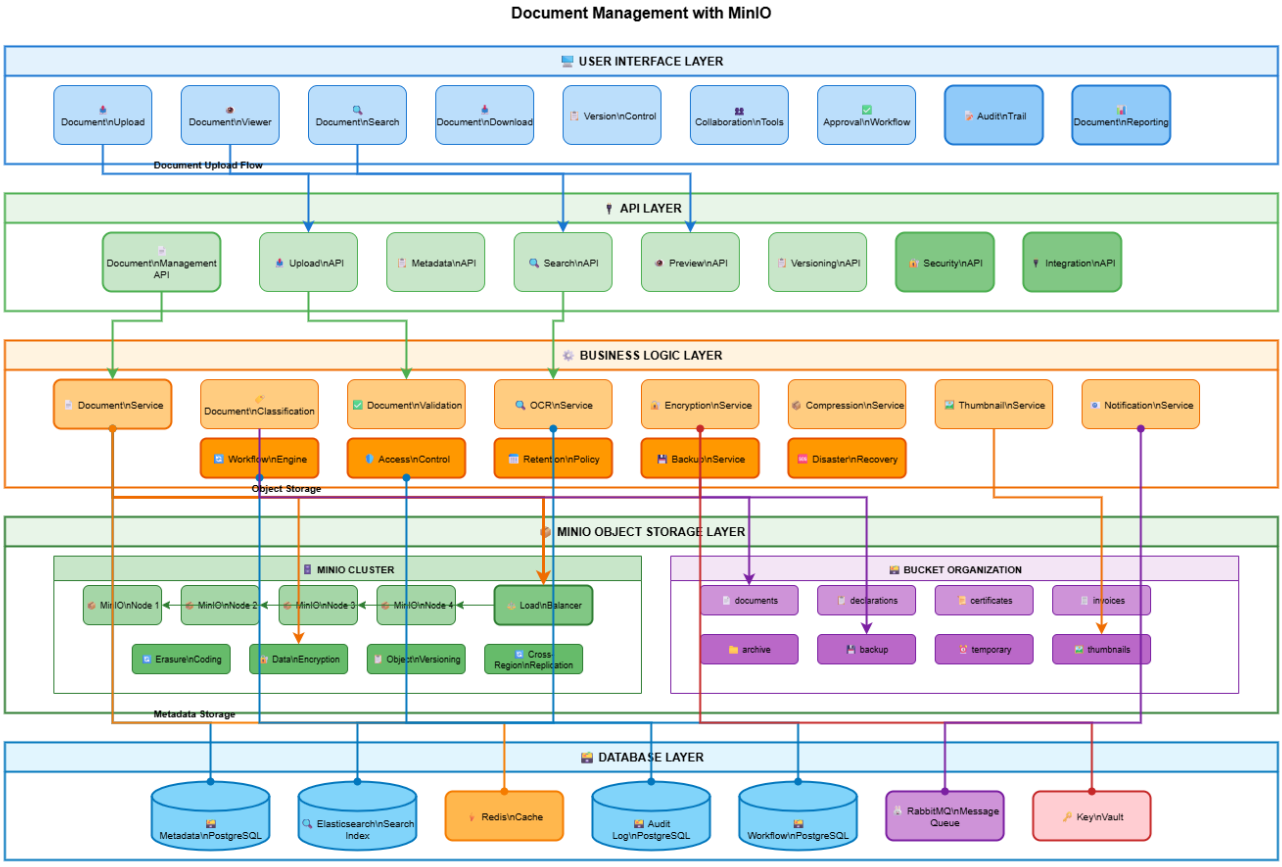
11.1.4 External system integrations



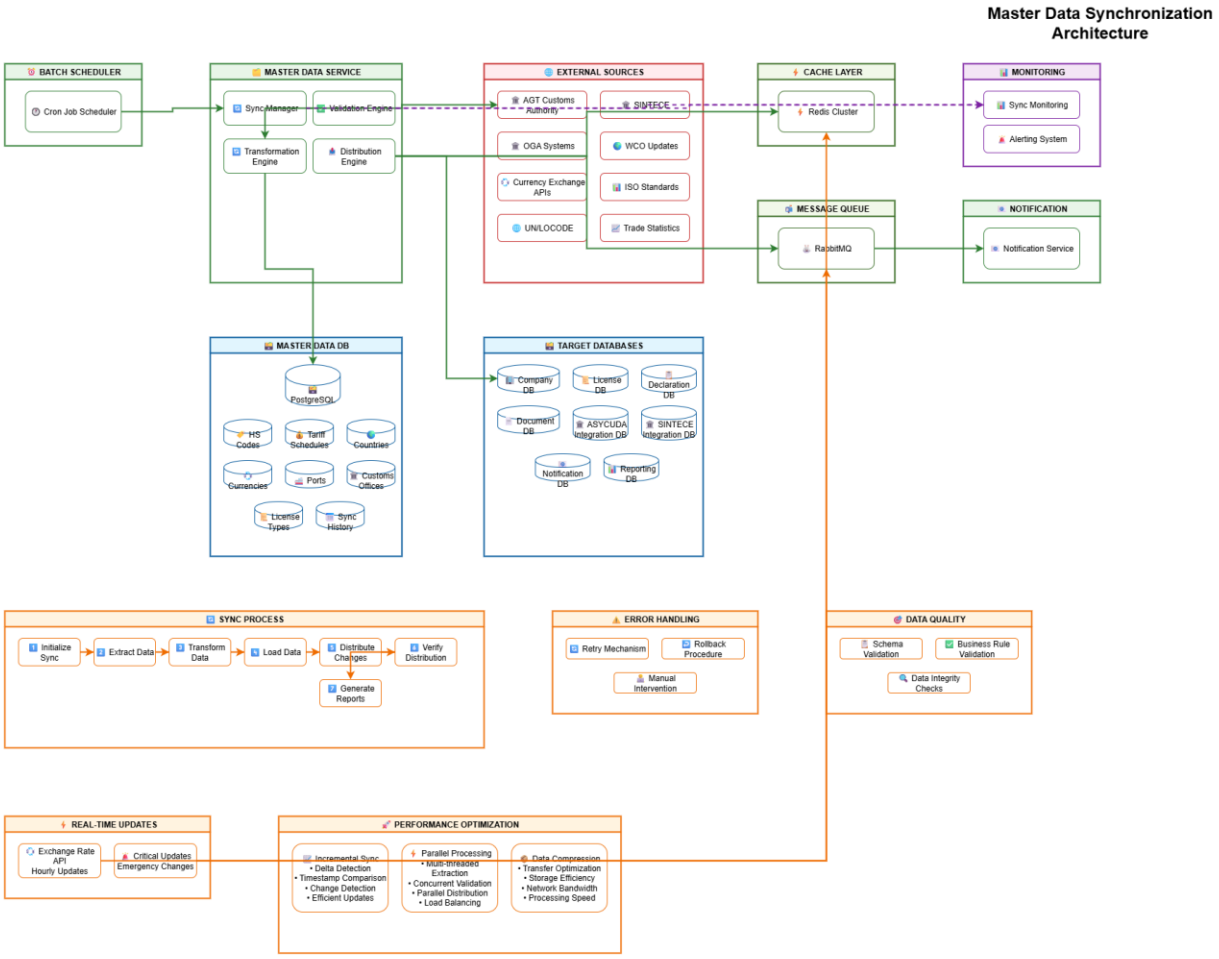
- Identity management architecture



11.1.5 Document storage architecture



11.1.6 Master data synchronization



11.2 Appendix B: Reference Documents

- JUL-AGT Integration Control Document - Draft - V2
- JUL-SINTECE Integration Control Document - Draft - v2
- JUL System User Management Architecture
- WCO Data Model Version 3.10
- UN/EDIFACT Message Standards
- UNCTAD Single Window Recommendations
- WTO Trade Facilitation Agreement Guidelines

11.3 Appendix C: Service Level Agreements

Metric	Target	Measurement
System Availability	99.9%	8.76 hours downtime/year maximum
API Response Time	< 3 seconds	95th percentile of all requests
Throughput	100 TPS	Sustained transaction processing rate

Recovery Time	< 4 hours	RTO for disaster recovery scenarios
Data Loss	< 1 hour	RPO for backup and recovery