Vodacom RPA Solution - Security & Implementation Roadmap

Contractor Delivery Status & Outstanding Requirements

🎯 Project Overview

Objective: Automated service validation and cancellation across multiple Fixed Network Operators (FNOs)
Client: Vodacom South Africa
Architecture: Orchestrator + Distributed Workers + Portal Automation

📊 Current Implementation Status

Use Case	Provider	Status	Validation	Cancellation	Target Date
✅ **UC1**	**MetroFiber (MFN)**	**COMPLETE**	✅ Live	✅ Live	**Delivered**
🔄 **UC2**	**Openserve (OSN)**	**QA Testing**	🧪 Testing	🧪 Testing	**2 Jul 2025**
🚧 **UC3**	**Octotel**	**Development**	🔧 In Dev	🔧 In Dev	**15 Jul 2025**
❓ **UC4**	**TBD**	**Specification**	📋 Planning	📋 Planning	**Aug 2025**

🔒 Security Implementation Status

✅ COMPLETED Security Features

- **Authentication:** JWT-based with configurable expiration
- **Authorization:** Role-based access with permission checking
- **Rate Limiting:** IP/API key based protection (1000 req/hour default)
- **Input Validation:** Pydantic models with SQL injection protection
- **Audit Logging:** Security events with correlation IDs
- **Network Security:** IP whitelisting for worker nodes
- **SSL/TLS:** Production-ready encryption
- **Error Handling:** No information disclosure on failures

🚨 OUTSTANDING Security Requirements

Critical Priority (Pre-Production)

1. **CyberArk Integration**
   - Replace config-based credentials with CyberArk vault calls
   - Implement automatic credential rotation

    - Secure portal authentication for all FNO providers

2. **Data Encryption at Rest**
    - Encrypt customer data in SQLite database
    - Secure screenshot storage (currently base64 in DB)
    - Evidence file encryption

3. **POPI Act Compliance**
    - Data retention policies (30-day default needs review)
    - Customer data anonymization for test environments
    - Right to be forgotten implementation

High Priority (Production Hardening)

4. **Enhanced Monitoring**
    - Security incident detection and alerting
    - Automation failure pattern analysis
    - Integration with Vodacom's SIEM systems

5. **Production Infrastructure**
    - Network segmentation (orchestrator ↔ workers)
    - VPN/private network requirements
    - Backup and disaster recovery procedures

📅 Implementation Roadmap

Phase 1: Security Hardening (2-3 weeks)

```
1-3 Jul: CyberArk Integration
- Replace all credential lookups with CyberArk API calls
- Implement credential rotation handling
- Test FNO portal authentication flows

8-12 Jul: Data Protection
- Implement AES encryption for customer data
- Secure evidence file storage
- POPI compliance review
```

Phase 2: Use Case Completion (3-4 weeks)

```
1-2 Jul: Openserve (OSN) QA Completion
- Fix validation edge cases (circuit not found scenarios)
- Optimize browser automation timeouts
- Complete cancellation flow testing

8-18 Jul: Octotel Development
- Portal reconnaissance and mapping
- Validation workflow implementation
- Cancellation workflow implementation

22 Jul-2 Aug: UC4 Specification & Planning
- FNO identification and portal analysis
- Technical feasibility assessment
```

Phase 3: Production Deployment (2-3 weeks)

```
5-16 Aug: Infrastructure Setup
- Production environment provisioning
- Network security implementation
- Monitoring and alerting setup

19-23 Aug: Go-Live Support
- Production deployment
- User training and handover
- Incident response procedures
```

⚠️ Key Risks & Mitigation

Risk	Impact	Mitigation
CyberArk Integration Delays	High	Early engagement with Vodacom security team
OSN Portal Changes	Medium	Robust element detection with fallback strategies
POPI Compliance Gaps	High	Legal review of data handling procedures
Network Connectivity Issues	Medium	Redundant worker deployment across regions

---

💰 Resource Requirements

Technical Resources

- **1x Senior Developer** (CyberArk integration + security hardening)
- **1x RPA Developer** (Octotel + UC4 development)
- **0.5x DevOps Engineer** (Infrastructure + monitoring)

Vodacom Dependencies

- **CyberArk vault access** and API credentials
- **Network connectivity** between orchestrator and FNO portals
- **Security review** and penetration testing
- **Production infrastructure** sizing and provisioning

🎯 Success Criteria

Technical

- ✅ All 4 use cases operational with 99% uptime
- ✅ Sub-5 minute automation execution time per job
- ✅ Zero data breaches or security incidents
- ✅ POPI Act compliance certification

Business

- ✅ 80% reduction in manual validation/cancellation effort
- ✅ Real-time status reporting to Vodacom systems
- ✅ Audit trail for regulatory compliance
- ✅ Scalable architecture for additional FNO providers

Next Steps: CyberArk integration workshop + OSN QA completion sprint
Review Date: Weekly roadmap updates
Escalation: Critical blockers to Vodacom project sponsor within 24h