

FEATURE_01 REVIEW GUIDE

December 16, 2025 at 10:30 AM

Feature #1 Implementation Plan - Review Guide

Purpose: Structured review of FEATURE_01_IMPLEMENTATION_PLAN.md before implementation begins

1. SCOPE & TIMELINE

What's Proposed

Timeline: 3 weeks (15 business days) - Week 1 (Days 1-5): Foundation - Week 2 (Days 6-10): Database & Export - Week 3 (Days 11-15): Migration & Testing

Developers: 1 full-time OR 2 part-time

Total Code: ~1,000 lines of new R code + tests

Review Questions

Q1.1: Is 3 weeks realistic for your environment?

- [OK] Yes, sounds right
- [TIME] Too aggressive, need 4-5 weeks
- [CONSIDER] Depends on developer experience level
- [NO] No specific timeline needed

Comments: _____

Q1.2: Developer allocation preference?

- [PERSON] 1 developer full-time (focused, no context-switching)
- [TEAM] 2 developers part-time (can parallelize modules)
- [FLEXIBLE] Flexible, depends on availability
- [OTHER] Other approach: _____

Comments: _____

2. MODULES & CODE STRUCTURE

What's Proposed

4 New R Modules (plus setup script + tests):

```
R/encryption_utils.R      (250-300 lines)
- generate_db_key()      : Create 256-bit random key
- verify_db_key()        : Validate key format
- test_encryption()      : Test encryption working
- get_encryption_key()   : Retrieve from env or AWS KMS
- get_encryption_key_from_aws_kms() : AWS integration

R/aws_kms_utils.R        (250-300 lines)
- setup_aws_kms()         : Configure AWS KMS
- rotate_encryption_key() : Re-encrypt with new key
- check_aws_kms_status() : Health check

R/secure_export.R          (300+ lines)
- secure_export_data()    : Export CSV/XLSX/SAS
- verify_export_integrity() : Hash verification
- anonymize_data()        : Remove identifiers

R/audit_logging.R           (200+ lines)
- log_audit_trail()       : Log every operation
- get_audit_trail()        : Query audit records
- generate_audit_report() : Create reports

setup_encrypted_database.R (100+ lines)
- setup_encrypted_database() : Fresh encrypted DB creation
```

Review Questions

Q2.1: Module breakdown - any changes?

- [OK] Looks good as-is
- [REORGANIZE] Consolidate some modules (fewer files)
- [SPLIT] Split into more focused modules
- [CONSIDER] Suggest different organization: _____

Comments: _____

Q2.2: Priority on which modules to create first?

- [1] encryption_utils.R (foundation, blocking others)
- [1] aws_kms_utils.R (optional, can defer)
- [1] secure_export.R (nice-to-have, business value)
- [1] audit_logging.R (critical for compliance)

Ranking (1=highest priority): _____

Comments: _____

Q2.3: Should we include all functions shown, or start minimal?

- [OK] Include all as shown (comprehensive)
- [TESTING] Start with core functions only, add others later
- [MINIMAL] Minimal set: _____

Comments: _____

3. KEY DEPENDENCIES & RISKS

External Dependencies

Required: - openssl (key generation) - Already in system - RSQLite >= 2.2.18 (database connection) - Already in DESCRIPTION - SQLCipher binary (encryption) - Platform-specific install

Optional: - paws (AWS KMS integration) - Only if using AWS - openxlsx (XLSX export) - Only for XLSX format - digest (file hashing) - Already in system

Review Questions

Q3.1: Acceptable to make paws and openxlsx optional?

- [OK] Yes, graceful degradation is fine
- [NO] No, they should be required
- [CONSIDER] Need conditional logic: _____

Comments: _____

Q3.2: Biggest implementation risk?

- [CRITICAL] SQLCipher installation across platforms
- [MEDIUM] AWS KMS integration complexity
- [MEDIUM] Export functionality edge cases
- [MEDIUM] Audit trail performance at scale
- [CONSIDER] Other: _____

Risk Mitigation: _____

Comments: _____

4. DATABASE SCHEMA CHANGES

What's Proposed

New Table: audit_trail

```
CREATE TABLE audit_trail (
    audit_id INTEGER PRIMARY KEY AUTOINCREMENT,
    timestamp TEXT NOT NULL,
    user_id TEXT NOT NULL,
    action TEXT NOT NULL,
    details TEXT, -- JSON with context
    status TEXT CHECK(status IN ('SUCCESS', 'FAILED', 'WARNING')),
    error_message TEXT,
    created_date TEXT DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_audit_timestamp ON audit_trail(timestamp);
CREATE INDEX idx_audit_user ON audit_trail(user_id);
CREATE INDEX idx_audit_action ON audit_trail(action);
CREATE INDEX idx_audit_status ON audit_trail(status);
```

No other changes - Encryption is transparent

Review Questions

Q4.1: Audit trail schema - any modifications?

- [OK] Looks good as-is
- [CHANGE] Add fields: _____
- [REMOVE] Remove fields: _____
- [CHANGE] Change design: _____

Comments: _____

Q4.2: Data retention policy for audit trail?

- [FOREVER] Keep forever (safest)
- [ROTATE] Rotate quarterly (current year + 3 years)
- [ROTATE] Rotate annually (rolling 7 years)
- [CONSIDER] Other: _____

Comments: _____

Q4.3: Should audit trail itself be encrypted?

- [OK] Yes (already encrypted with database)
- [NO] No, separate unencrypted audit log
- [CONSIDER] Depends on: _____

Comments: _____

5. TESTING STRATEGY

What's Proposed

15+ Test Cases organized by category:

Unit Tests:

- Key generation (2 tests)
- Key verification (2 tests)
- Encryption (2 tests)
- Export (1 test)
- Audit trail (1 test)

Integration Tests:

- Full workflow (1 test)
- Multiple operations (1 test)
- Key rotation (1 test)

Security Tests:

- Encryption verification (1 test)
- Wrong key rejection (1 test)

Performance Tests:

- Connection overhead (1 test)

Review Questions

Q5.1: Test coverage - sufficient?

- [OK] Yes, good coverage
- [TESTING] Add more tests for: _____
- [FOCUS] Focus on: _____
- [PERFORMANCE] Performance tests more critical

Comments: _____

Q5.2: Should we include stress testing?

- [OK] Yes, test with large datasets (10K+ records)
- [DEFER] No, defer to Phase 2 performance testing
- [CONSIDER] Include if time permits

Comments: _____

Q5.3: CI/CD testing requirements?

- [OK] All tests must pass before merge
- [WARNING] Some tests can be optional
- [REVIEW] Manual security review required
- [DEFER] Testing happens after deployment

Comments: _____

6. DOCUMENTATION & DEPLOYMENT

What's Proposed

3 Documentation Files: 1. vignettes/feature-encryption-at-rest.Rmd - User guide 2. documentation/ENCRYPTION_DEPLOYMENT_GUIDE.md - Production deployment 3. documentation/ENCRYPTION_TROUBLESHOOTING.md - Common issues

Coverage: - Setup instructions (all 3 trial scenarios) - Key management (generation, storage, rotation) - AWS KMS configuration - Export procedures - Audit trail usage - Troubleshooting

Review Questions**Q6.1: Documentation scope - sufficient?**

- [OK] Yes, covers all scenarios
- [ADD] Add guidance on: _____
- [REMOVE_DOC] Skip: _____

Comments: _____

Q6.2: Who needs training?

- [PERSON] DBAs (key management)
- [PERSON] Data managers (export procedures)
- [PERSON] System admins (AWS KMS setup)
- [PERSON] Developers (integration code)
- [CONSIDER] Create training plan?

Comments: _____

Q6.3: Deployment checklist - include?

- [OK] Yes, pre-deployment checklist (database backup, key setup, etc.)
- [NO] No, assume manual verification
- [CONSIDER] Create automated pre-deployment validation script?

Comments: _____

7. INTEGRATION WITH EXISTING CODE

What's Proposed

Modified Files: - global.R - Add get_db_connection(), close_db_connection() - server.R - Initialize encrypted connection - data.R - All DB access through encrypted connection - export.R - Use secure_export_data() - DESCRIPTION - Add openssl dependency

Non-Breaking Changes: - Fresh database start (no migration) - All SQL unchanged (SQL-Cipher transparent) - Existing queries continue working

Review Questions

Q7.1: Fresh database start - acceptable?

- [OK] Yes, we want clean encryption from day 1
- [NO] No, must preserve existing data
- [CONSIDER] Need migration path: _____

Comments: _____

Q7.2: Changes to global.R, server.R, data.R

- [OK] Minimal changes shown are good
- [CHANGE] Prefer different approach: _____
- [WARNING] Concerned about: _____

Comments: _____

Q7.3: Breaking changes acceptable?

- [OK] Yes, this is a breaking change, users understand
- [WARNING] Prefer gradual migration
- [CONSIDER] Need backwards compatibility: _____

Comments: _____

8. SUCCESS CRITERIA

What's Proposed

Feature #1 Complete When:

1. [OK] **Encryption Working**
 - SQLCipher integrated, transparent encryption active
 - All data stored encrypted (verified by file inspection)
 - Performance overhead < 5%
 2. [OK] **Key Management**
 - 256-bit keys auto-generated
 - Environment variable storage working (dev)
 - AWS KMS integration working (production)
 - Key rotation procedure documented and tested
 3. [OK] **Secure Export**
 - CSV/XLSX/SAS export functionality working
 - Anonymization option working
 - File integrity hash verification working
 4. [OK] **Audit Trail**
 - Every DB connection logged
 - Every query/export logged
 - Audit records immutable (append-only)
 5. [OK] **All Tests Passing**
 - 15+ unit/integration tests all pass
 - Security tests verify encryption
 - Performance tests < 5% overhead
 6. [OK] **Documentation Complete**
 - User guide for all 3 trial scenarios
 - Production deployment guide
 - Troubleshooting guide
 - Code examples
 7. [OK] **GDPR/FDA Compliance**
 - Article 32 encryption at rest
 - 21 CFR Part 11 audit trail
 - All applicable articles covered
-

Review Questions

Q8.1: Success criteria - complete?

- [OK] Yes, covers all important aspects
- [ADD] Add criteria for: _____
- [REMOVE] Remove: _____

- [CHANGE] Modify: _____

Comments: _____

Q8.2: Performance targets acceptable?

- [OK] < 5% overhead is good target
- [STRICT] Should be < 2%
- [TIME] < 5% might be tight, use < 10%
- [PERFORMANCE] Skip performance testing initially

Comments: _____

Q8.3: Regulatory compliance verification?

- [PERSON] Manual review by compliance team
- [OK] Automated compliance checklist
- [OTHER] Both (automated + manual review)
- [WHO] Who verifies?

Comments: _____

9. OVERALL QUESTIONS

Q9.1: Proceed with implementation as planned?

- [OK] Yes, start immediately (no changes)
- [WITH_CHANGES] Yes, with modifications (see below)
- [CONSIDER] Need more time to review
- [NO] No, major changes needed
- [DEFER] Defer to Phase 2

Modifications needed (if yes with changes): _____

Q9.2: Any blockers or concerns?

Q9.3: Resource allocation confirmed?

- [OK] 1 developer available full-time, starting [DATE]
- [OK] 2 developers available part-time, starting [DATE]
- [TIME] Availability unclear, need to confirm
- [NO] No developers available yet

Dates/names: _____

Q9.4: Key contact for questions during implementation?

Name: _____ **Role:** _____ **Email/Phone:** _____ **Timezone:** _____

IMPLEMENTATION START CHECKLIST

Once you complete this review, we'll verify:

- All review questions answered
- Any adjustments documented
- Developer(s) assigned and confirmed
- Timeline agreed upon
- Success criteria approved
- Resources confirmed

Then: Begin Step 1 (SQLCipher installation) in Week 1, Day 1

Ready to complete this review guide?