Design Assumptions

Business Rules

1. Citizens must be 18+ years old
2. Each citizen can have only ONE active digital ID
3. Consent expires after 1 year unless renewed
4. Authorization for entities expires annually

Data Retention

- Audit logs retained for 7 years (compliance)
- Expired requests purged after 2 years
- Citizen data retained indefinitely unless deleted

Security Assumptions

- Biometric data encrypted at rest using AES-256
- Database connections use TLS/SSL
- Access logs are immutable (no updates/deletes)

Operational Assumptions

- System available 24/7 except during maintenance
- Weekday DML restriction applies Mon-Fri only
- Holidays checked before any INSERT/UPDATE/DELETE
- High-risk requests (risk_score > 0.7) require manual review

Normalization

- All tables in 3NF minimum
- No redundant data across tables
- Foreign keys enforce referential integrity