x509 Certificate Validation Test Strategy and Automation

1. Testing Scope & Objectives

Key attributes to validate:

- **Common Name (CN)**
- **Issuer details**
- **Validity dates (Not Before, Not After)**
- **Signature algorithm (RSA 2048+, SHA-256+)**

Why certificate integrity matters:

- Prevents man-in-the-middle (MITM) attacks.
- Validates trust chain for secure communication.
- Ensures certificate has not expired or been tampered with.

2. Manual vs Automated Testing

Manual Testing:

- Visual inspection of certificates (using OpenSSL) for one-off scenarios.
- Revocation verification using external tools.
- Checking UI displays (in browsers or applications).

Automated Testing:

- Certificate generation validation.
- Structure parsing & validation of CN, issuer, expiry.
- Signature algorithm checks.
- Automated negative tests (expired, malformed, revoked certs).
- Performance and validation time measurements.
- Data-driven testing with multiple certificates.

3. Test Scenarios

Positive Cases:

- Certificate with correct CN, issuer, expiry.
- Strong signature algorithm (RSA 2048, SHA-256).

Negative Cases:

- Expired certificate.
- Weak signature algorithms (MD5, SHA1).
- Malformed or incomplete certificates.
- Revoked certificates detected via CRL or OCSP.

Edge Cases:

- Unsupported encryption algorithms.
- Certificates with very short expiry.
- Certificates missing critical extensions.

4. Automation Strategy

- **Tools:**
  - OpenSSL (for certificate creation and manipulation)
  - Java KeyStore API / Bouncy Castle (for parsing and advanced validation)
  - TestNG (for test execution framework)
- **Test Data:**
  - Store multiple certificates (valid, expired, malformed, revoked) in `src/test/resources`.
  - Use TestNG's `@DataProvider` to iterate over certificates.
- **Validation Logic:**
  - Parse certificates and assert conditions dynamically.
  - Report failures with detailed diagnostics.

5. Security & Performance Considerations

- Enforce strong cryptographic standards (RSA 2048+, SHA-256 or ECDSA).
- Automatically reject deprecated algorithms.
- Monitor and log certificate parsing/validation duration.
- Include checks for certificates revoked