## Documentation of Implementation Security Properties

1. **RSA Key Management**
    - Uses **2048-bit RSA keys** for strong security.
    - Saves keys in **PEM format** to ensure compatibility.
    - **Private keys must be protected** (e.g., stored securely and not shared).
2. **Asymmetric Encryption Security**
    - Uses **OAEP padding with SHA-256**, ensuring resistance to attacks.
    - Encrypts messages securely using the public key.
    - Only the **private key** can decrypt the message.
3. **PKI Security Considerations**
    - Uses **self-signed certificates** (not trusted by default in browsers).
    - Certificates can be distributed to establish trust.
    - Can be extended to use **Certificate Authorities (CA)**.
4. **Secure Key Exchange**
    - Symmetric key is securely transmitted using RSA encryption.
    - Prevents interception of the symmetric key during exchange.
    - Ensures confidentiality in encrypted communications.