

[Mobile Application and Architecture Considerations](#) from *The Open Web Application Security Project* is available under a [Creative Commons Attribution-ShareAlike 3.0 Unported](#) license.

Mobile Application and Architecture Considerations

Use this document to review the various architecture considerations for mobile applications and architecture.

Note: Not all of the following may apply to your mobile app. You will need to address only those areas that apply to the particular application you have chosen.

1. What is the design of the architecture (network infrastructure, web services, trust boundaries, third-party APIs, etc.)?
 - o Carrier
 - Data
 - SMS
 - Voice
 - o Endpoints
 - Web Services
 - RESTful or SOAP-based
 - Third Party (Example: Amazon)
 - Websites
 - Does the app use or integrate the “mobile web” version of an existing web site?
 - App Stores
 - Google Play
 - Apple App Store
 - Windows Mobile
 - BlackBerry App Store
 - Cloud Storage
 - Amazon/Azure
 - Corporate networks (via VPN, SSH, etc.)
 - o Wireless interfaces
 - 802.11
 - NFC
 - Bluetooth
 - RFID
 - o Device

- App layer
 - Runtime environment (VM, framework dependencies, etc.)
 - OS platform
 - Apple iOS
 - Android
 - Windows Mobile
 - BlackBerry
 - Baseband
- 2. What are the common hardware components?
 - GPS
 - Sensors (accelerometer)
 - Cellular radios (GSM/CDMA/LTE)
 - Flash memory
 - Removable storage (i.e.- SD)
 - USB ports
 - Wireless interfaces
 - 802.11
 - Bluetooth
 - NFC
 - RFID
 - Touch screen
 - Hardware keyboard
 - Microphone
 - Camera
- 3. What are the authentication specifics?
 - Method
 - Knowledge-based
 - Token-based
 - Biometrics
 - Input Type
 - Keyboard
 - Touch screen
 - Hardware peripheral
 - Decision Process
 - Local (on device)
 - Remote (off device)
- 4. Define the app architecture relative to OS stack + security model
 - What should or shouldn't the app do?