



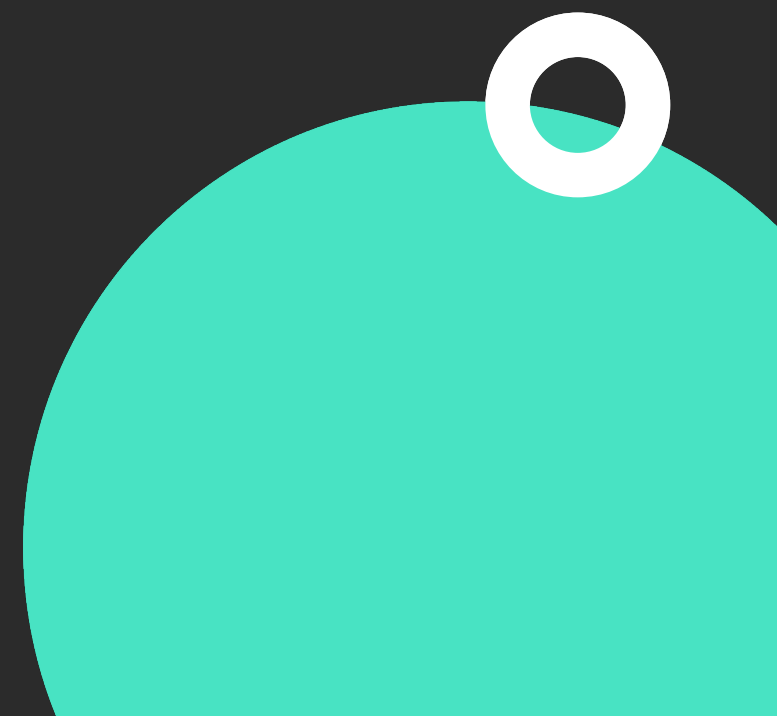
Perform public key pinning in KMM Project with Ktor



Hardik Trivedi

 @MrHardikTrivedi

 in/mrhardiktrivedi



Course rundown

- What is **Public key pinning**?
- Understanding the **requirement**
- High level **architecture**
- **Starter** project
- **Add support** for **public key pinning** in the project
- Coding **challenge** and **solution**



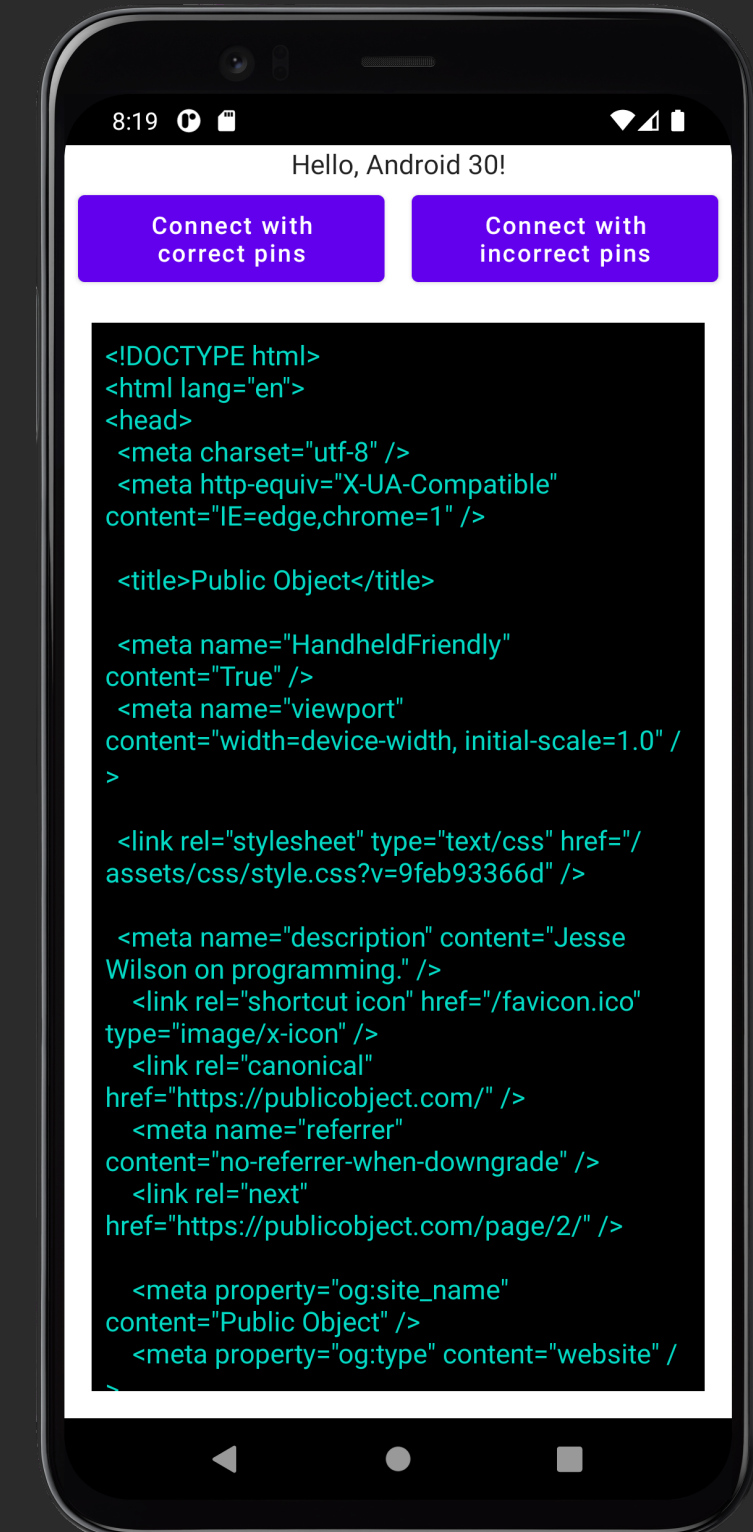
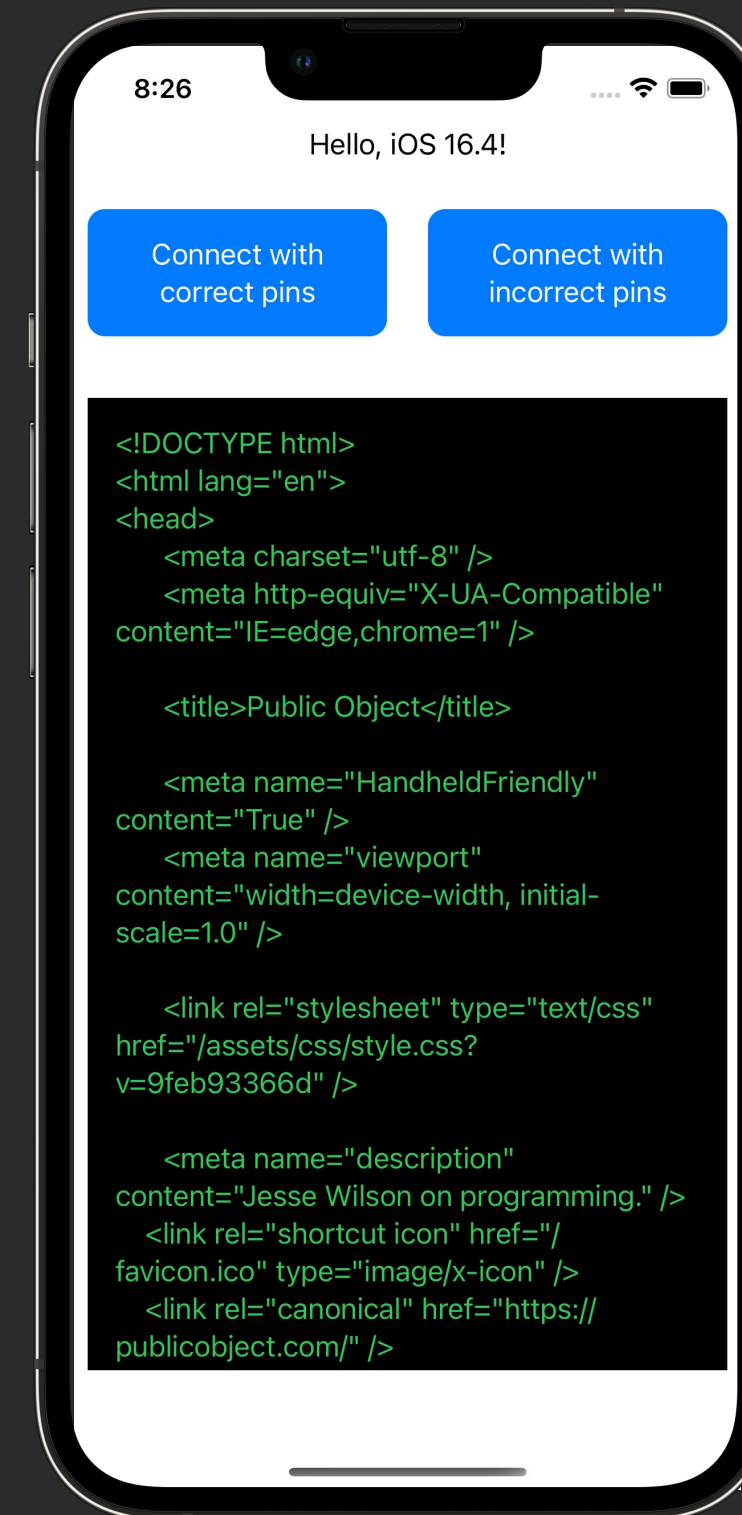
What is public key pinning?

- Public key pinning enhances security in mobile apps by ensuring connections are made only to trusted servers.
- It associates a mobile app's server public key with its domain, verifying server identity during the secure communication process.
- The mobile app includes pinned public keys in its configuration to enforce the policy.
- The app compares the server's public key with the pinned keys to detect unauthorized changes or interception attempts.
- Proper management, key rotation, and contingency plans are crucial to prevent disruptions or misconfiguration issues in the mobile app's security implementation

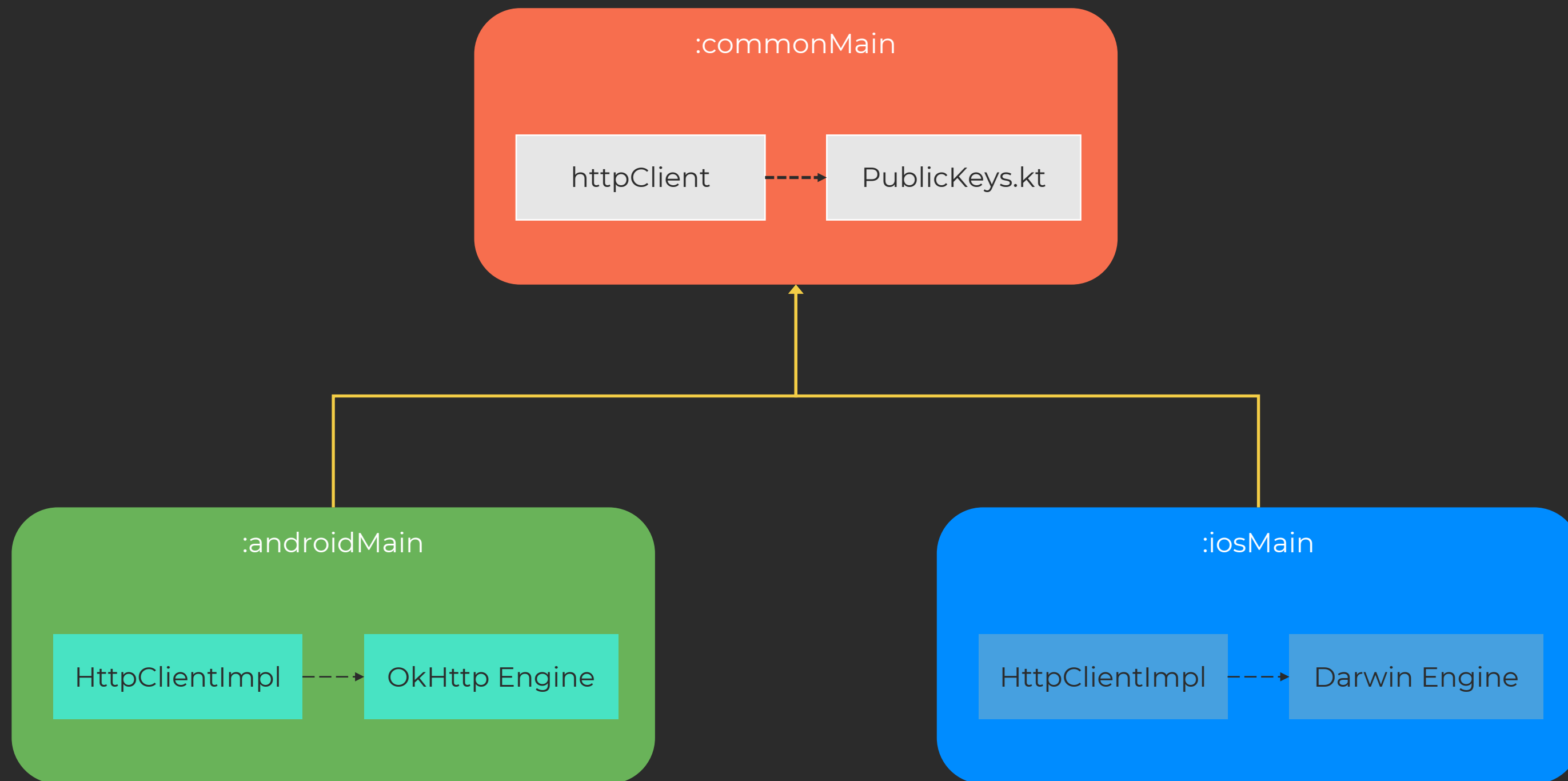


Understanding the requirement

- A multi-platform app using KMM which runs on both Android and iOS
- The app has two buttons to connect to <https://publicobject.com/>
- One button will try to connect with a valid set of public keys
- Another button will try to connect with an invalid set of public keys
- The app will display success response with green colour and failure response with red colour



High level architecture





Let's pull starter project

Up Next





Implementing a PinningService

Up Next





Adding pins

Up Next





Coding challenge

Up Next



Add support for an additional pins

- The **product owner** has asked you to **provide support for an additional pin** due to configuration changes on server side.
- New pin is **"sha256/C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M="**
- **How** would you do that?



Closure

- Sharing network layer in `KMM`
- Learned how to `safeguard` your `API` calls.
- Using `expect/actual` we can target platform specific implementation.
- Power of `Ktor engine`





Thank you



Hardik Trivedi

 @MrHardikTrivedi

 in/mrhardiktrivedi

