droidcon academy

Perform public key pinning in KMM Project with Ktor

Hardik Trivedi

@MrHardikTrivedi

in/mrhardiktrivedi

Course rundown

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

droidcon academy

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

What is KMM?

- KMM is an abbreviation that can stand for "Kotlin Multiplatform Mobile".
- It is a framework for mobile app development that allows developers to write a single codebase in the Kotlin programming language.
- Then it’s compiled into native code for different platforms such as iOS and Android.
- This means that developers can share code across multiple platforms
- Framework is developed by the JetBrains
- It is trusted in production by many of the world’s leading companies, including Philips, Netflix, Leroy Merlin, Cash App, and VMWare.

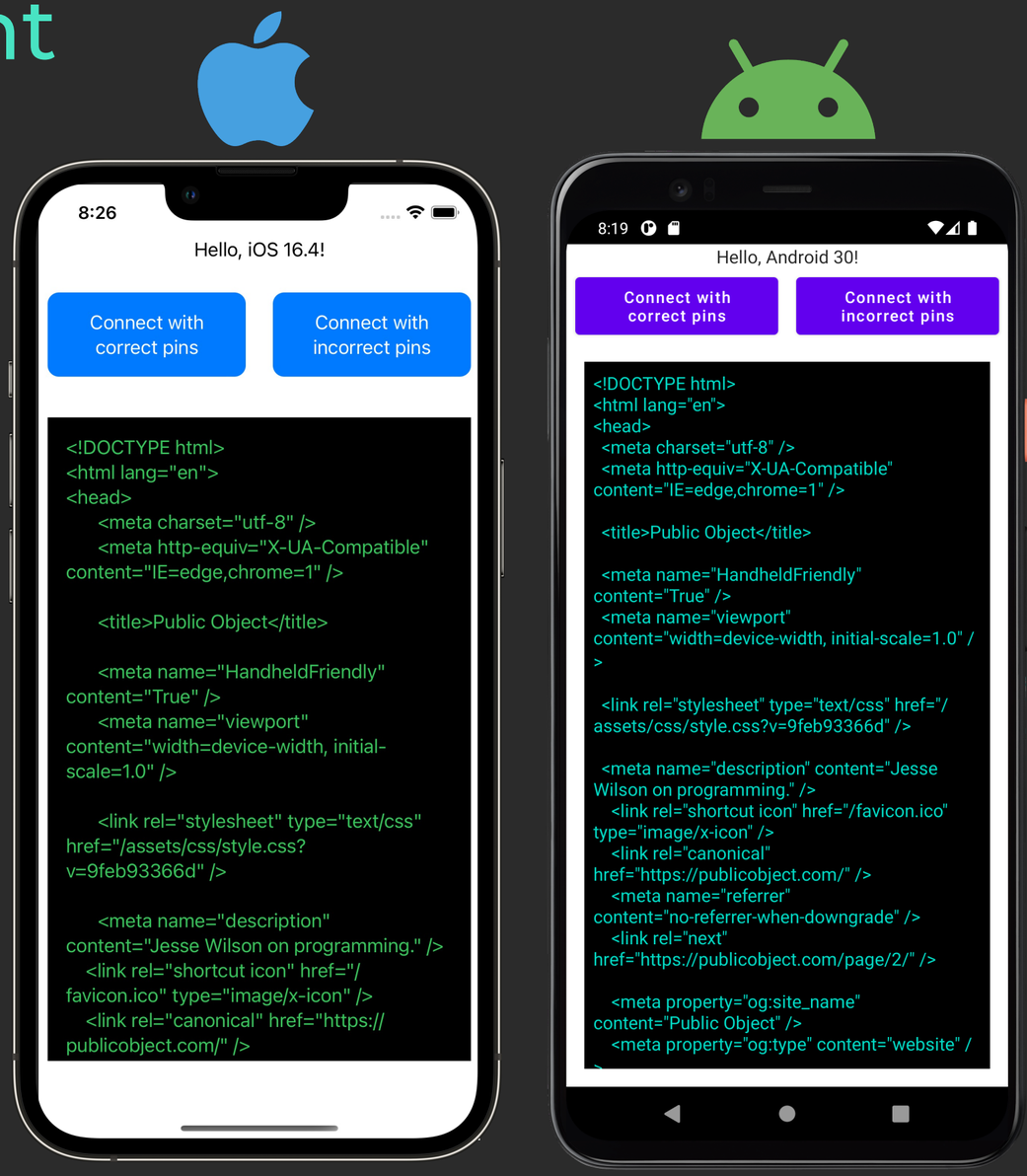
What is Ktor?

- Ktor is lightweight, async networking framework for Kotlin.
- Ideal for mobile KMM projects, enables shared networking code between Android and iOS.
- Simplifies HTTP requests, response handling, and WebSocket communication.
- Streamlines REST API development with routing, authentication, and serialization.
- Efficient and non-blocking with built-in coroutine support for fast, concurrent operations.

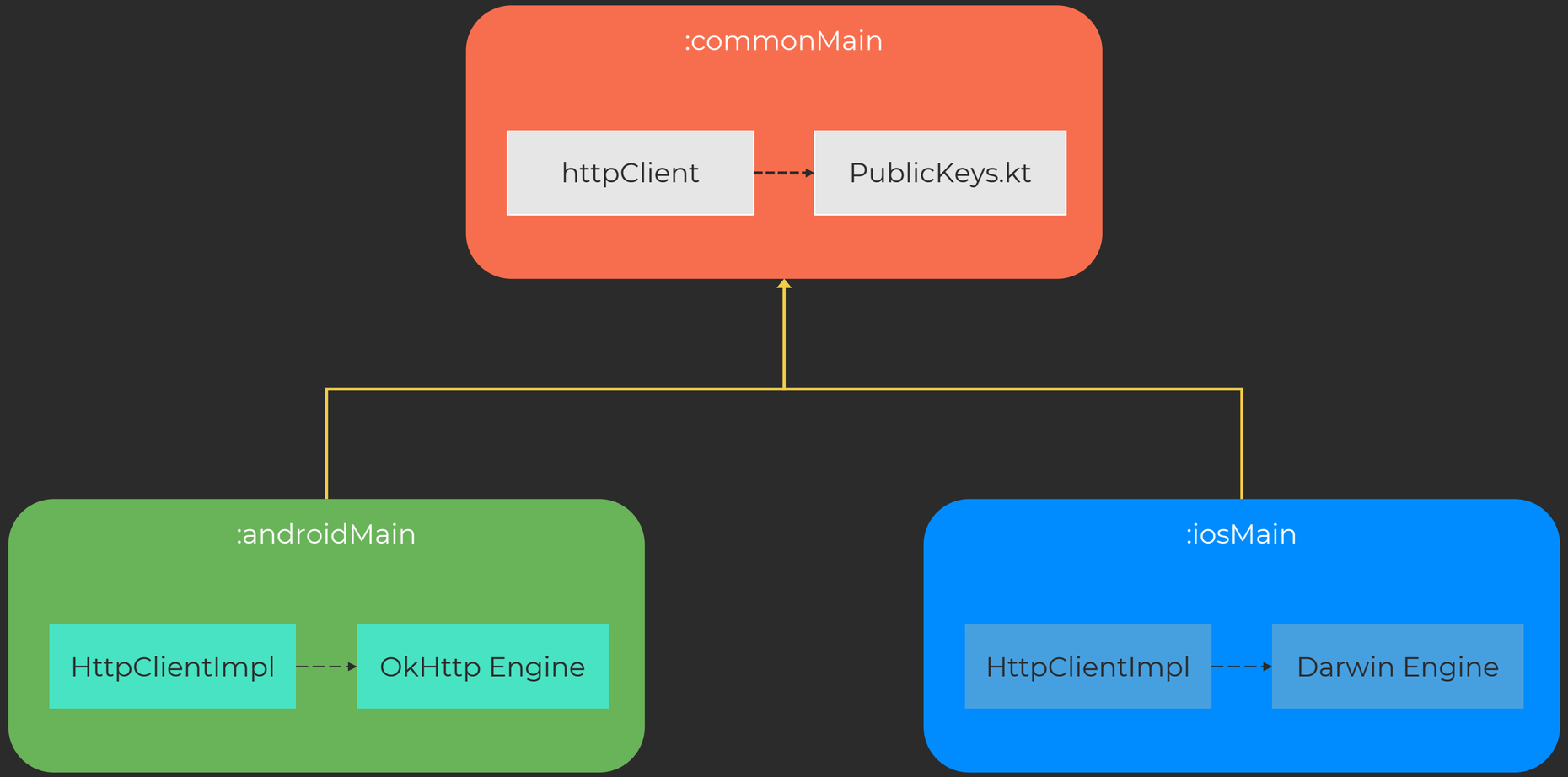
droidcon academy

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



droidcon academy

Let’s pull starter project

Up Next

droidcon academy

Implementing a PinningService

Up Next

droidcon academy

Adding pins

Up Next

droidcon academy

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

droidcon academy

droidcon academy

Thank you

Hardik Trivedi

@MrHardikTrivedi

in/mrhardiktrivedi