



Next Generation's  
**DIGITAL SIGNATURES**

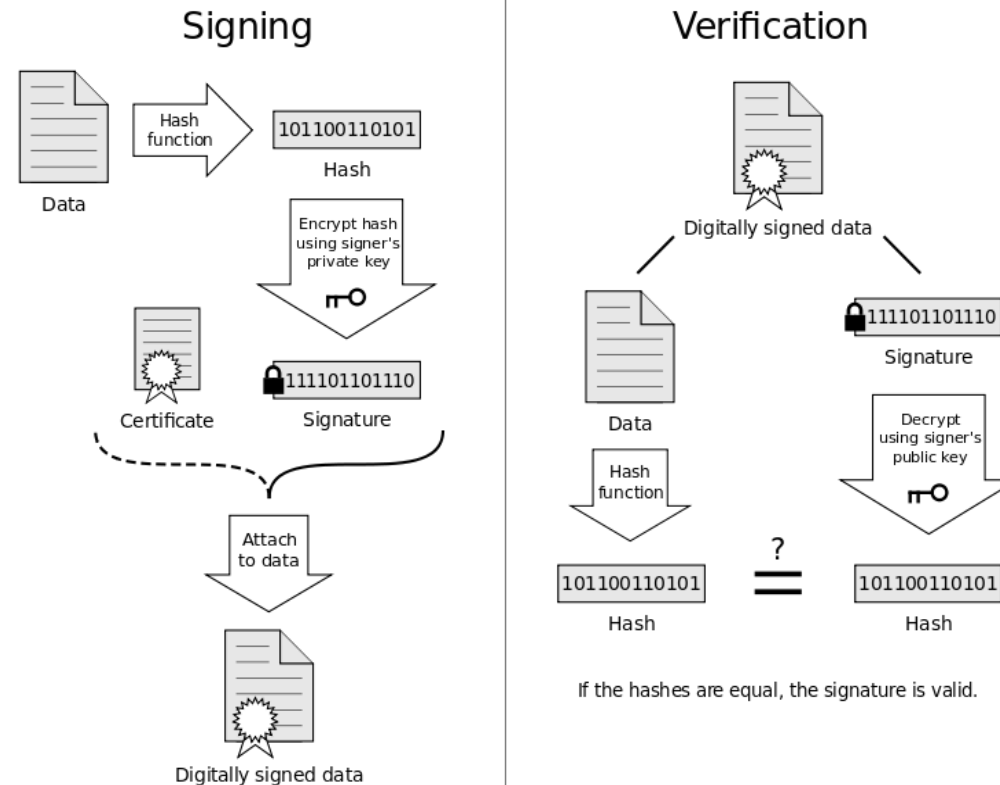


# DIGITAL SIGNATURES

- A digital signature is an **electronic, encrypted, stamp of authentication** on digital information
- A signature **confirms** that the information **originated from the signer.**
- **Legally accepted** Digital counterpart of a wet signature
- **Classes** are used to **Measure Validity.**
- Certificate Service Provider (**CSP**) of Sri Lanka – **Lanka Pay** is the **only legal body** authorized to provide **Class 3** certificates



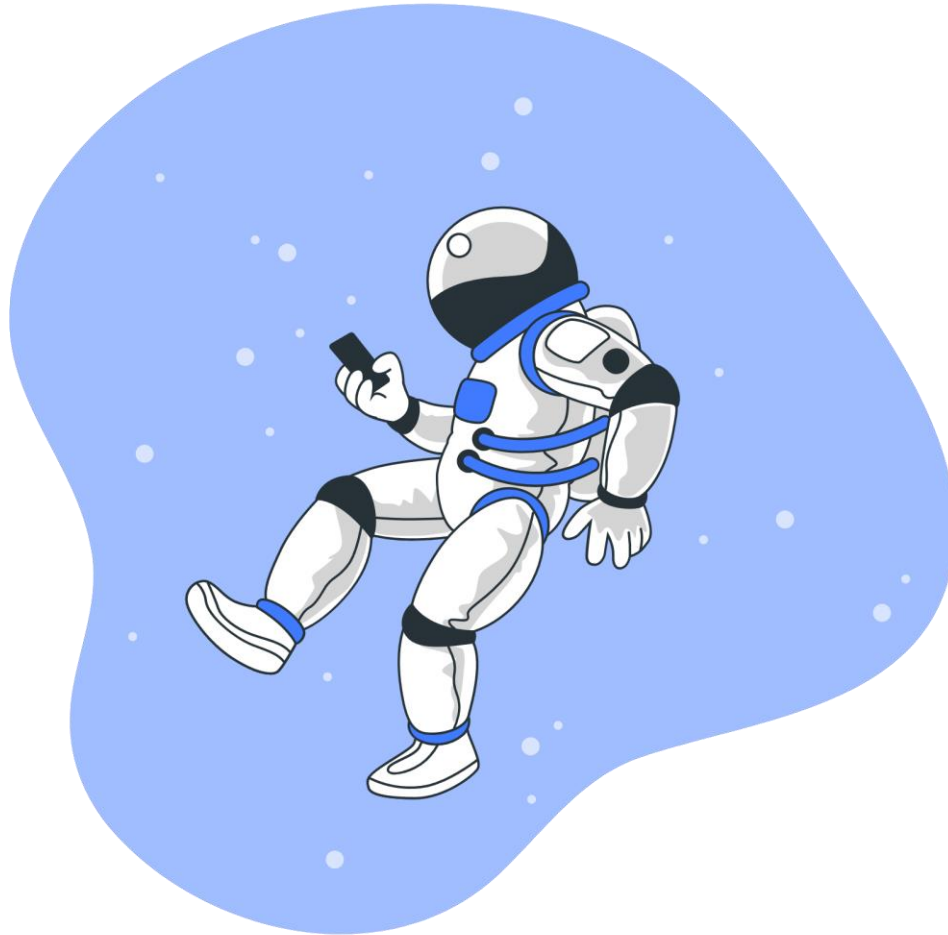
# The Process of Digitally Signing




The standard signing process where a hash is generated from the document and digitally signed with the user's private key

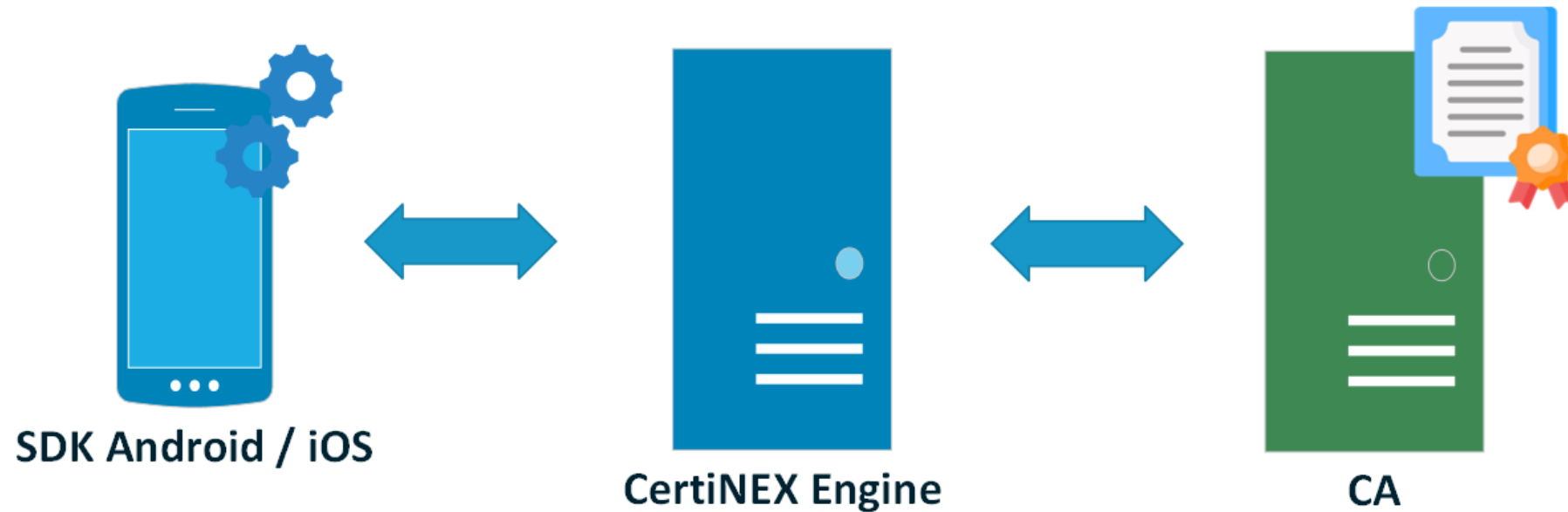
# Solution ?

---

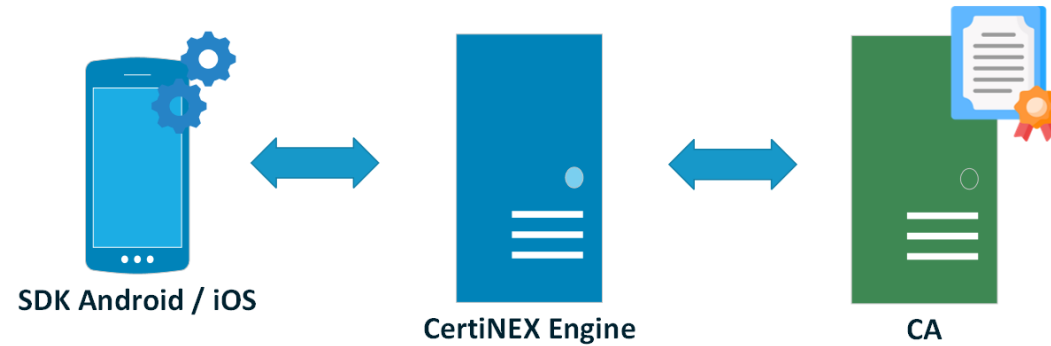


The solution is  **CertiNEX** , the only digital signature acquiring CA connector platform available in Sri Lanka.

# HIGHLEVEL ARCHITECTURE



The solution enables to connect to the **Certificate Authority** and **acquires a digital certificate** and delivers that to a **secure location in the mobile device**



The solution has 3 main components

Certificate Authority, **CertiNEX** Engine and Android and iOS **SDKs**

**CertiNEX** Engine functions as a highly secure innovative platform connecting with the Certificate Authority.

The engine is built using micro service architecture and is built on the Microsoft's Network Device Enrollment Service (NDES) and uses Simple Certificate Enrollment Protocol (SCEP) invented by SISCO.

**CertiNEX** Engine also comprises of a CA Admin module enabling Certificate functions, Namely Certificate Service Request (CSR) Accept & reject, Certificate revoke.

And advance back-office functions such as license management, device management and logs management.



Initiation

Enrollment

Sign

Renew

Revoke

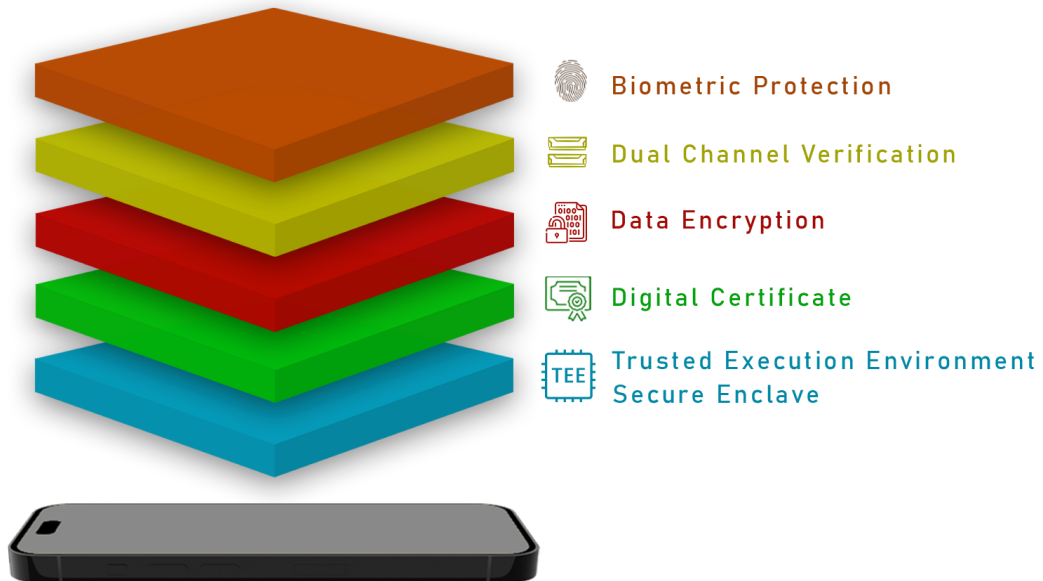
Public Cert

## CertiNEX Mobile SDK

- CertiNEX SDK has separate counterparts for both Android and iOS.
- Any organization can build certificate based mobile applications using this SDK as its backbone.
- CertiNEX will support all the certificate related functions such as enrollment and signing etc.

# MOBILE SECURITY LAYERS

CertiNEX SDK is developed to utilize the most advanced mobile security available in modern mobile devices.



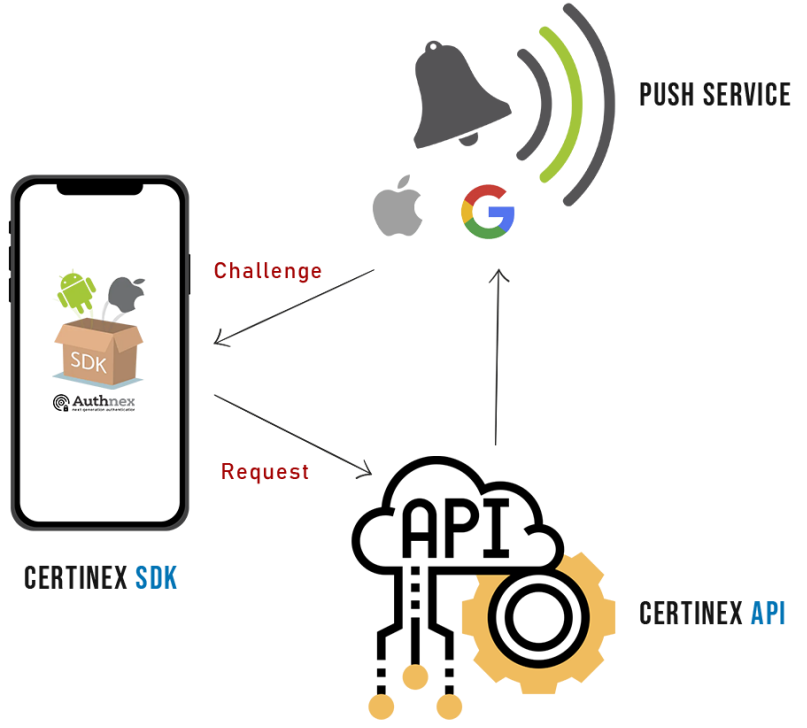
A **Trusted Execution Environment (TEE)** on Android and the **Secure Enclave** on IOS is an area that ensures data is stored, processed and protected in a separate secure environment even the device is rooted.

CertiNEX follows **Public Key Infrastructure (PKI)**, and the key pair is generated inside the secure elements and the signing functions are also executed inside the secure element itself

Moreover, CertiNEX secures the certificate using user biometrics.



# INNOVATIVE SECURITY



While securing data from inside the mobile, **CertiNEX** uses our **own inventive mechanism**, the **dual channel authentication** to verify the identity of the device. Preventing unidentified devices from penetrating the system.

## Dual Channel Authentication

# INCORPORATING WORLD CLASS SECURITY

## API & Communication



JWT Tokens



Token Based Authorizations



Hybrid Cryptosystem



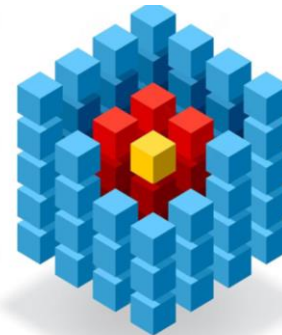
Scope Level Authorization



Logging & Monitoring



Digital Certificate



CertiNEX API Request/Response Body

 JWT Payload

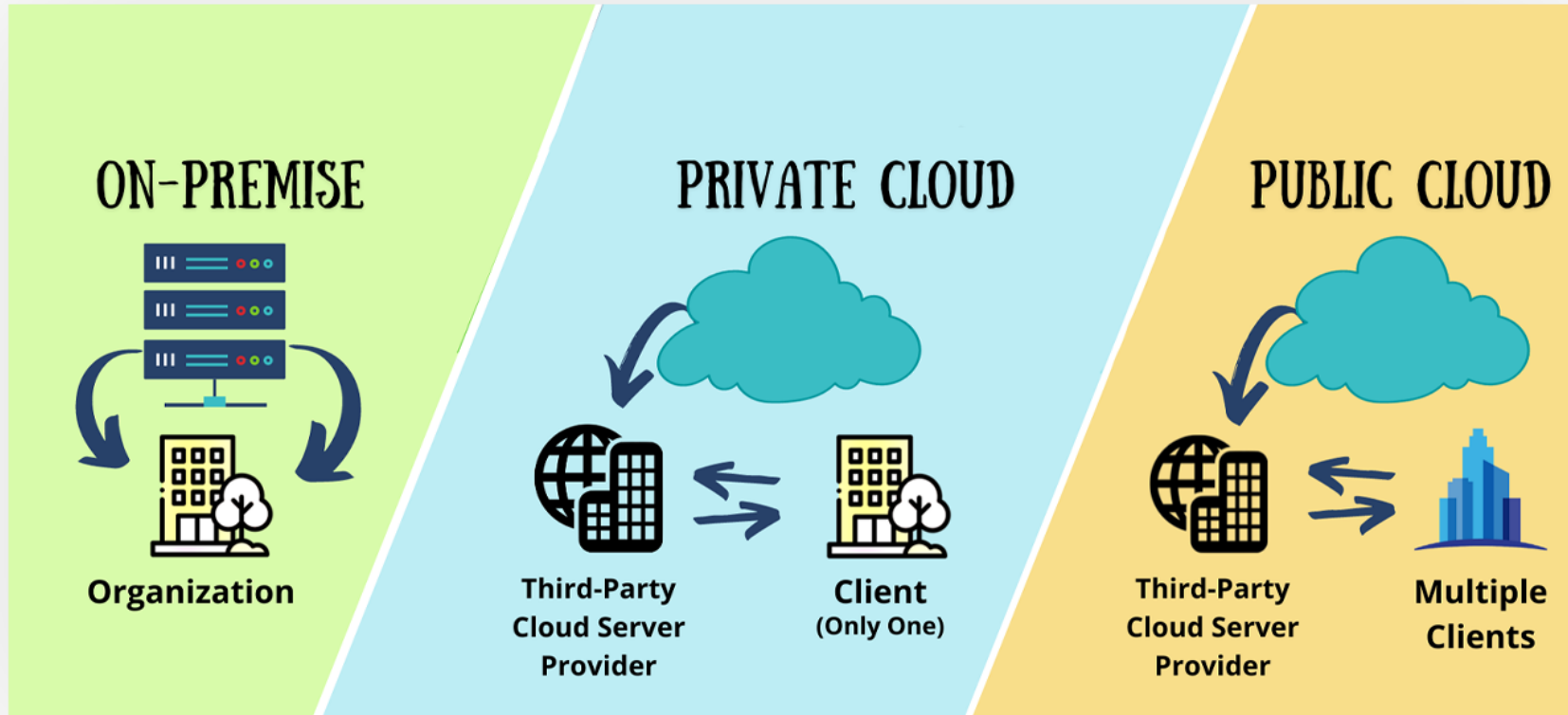
 Signed Payload

 Encrypted Payload

All **API communications** are **tokenized** according to the JWT standards

And **signed** and **encrypted** to prevent any interception

# IMPLEMENTATION



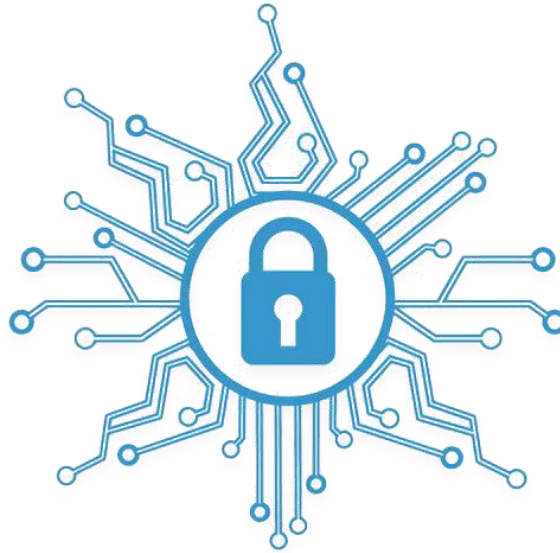
Windows



Mac



Linux



In conclusion, **CertiNEX** is a remarkable innovative endeavor providing Sri Lankas first, most versatile platform to **acquire, store** and **sign** digital certificates.

Utilizing highest grade technologies, ground-breaking innovations and frameworks to ensure speed stability and most of all security.