SSL PINNING GUIDELINE FOR WEB APPLICATION(S)

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

SSL Pinning Guidelines
FOR WEB BASED APPLICATIONS

SSL PINNING GUIDELINE

```
func urlSession(_ session: URLSession, didReceive challenge: URLAuthenticationChallenge, completionHandler:
@escaping (URLSession.AuthChallengeDisposition, URLCredential?) -> Void) {
    let serverTrust = challenge.protectionSpace.serverTrust
    let certificate =  SecTrustGetCertificateAtIndex(serverTrust!, 0)

    //set ssl polocies for domain name check
    let policies = NSMutableArray()
    policies.add(SecPolicyCreateSSL(true, challenge.protectionSpace.host as CFString))
    SecTrustSetPolicies(serverTrust!, policies)
```

SSL PINNING GUIDELINE(CONT'D)

```
//evaluate server certifiacte
    var result:SecTrustResultType =  SecTrustResultType(rawValue: 0)!
    SecTrustEvaluate(serverTrust!, &result)
    let isServerTRusted:Bool =  (result == SecTrustResultType.unspecified || result == SecTrustResultType.proceed)

    //get Local and Remote certificate Data

    let remoteCertificateData:NSData =  SecCertificateCopyData(certificate!)
    let pathToCertificate = Bundle.main.path(forResource: "github.com", ofType: "cer")
    let localCertificateData:NSData = NSData(contentsOfFile: pathToCertificate!)!

    //Compare certificates
    if(isServerTRusted && remoteCertificateData.isEqual(to: localCertificateData as Data)){
       let credential:URLCredential =  URLCredential(trust:serverTrust!)
       completionHandler(.useCredential,credential)
    }
    else{
       completionHandler(.cancelAuthenticationChallenge,nil)
    }
  }
```

THANK YOU