Mobile Federations Tools for OIDCfed

Elena Torroglosa (University of Murcia)

GÉANT OIDCFed Team (GN4-2 JRA3 Task 3 1.A)

TNC2018

Trondheim, June 14th, 2018

The OIDC Federation 1.0 – Draft 04

- http://openid.net/specs/openid-connect-federation-1_0.html
- Federation support happens in:
  - Dynamic discovery
  - Dynamic registration
- Applications have to support
  - Constructing a Signed Metadata Statement
  - Verifying the Metadata Statement
  - Flattening the Compounded Metadata Statement

AppAuth

- AppAuth is a client SDK for native apps to authenticate and authorize end-users
  - Using OAuth 2.0 and OpenID Connect
  - Available for iOS, macOS, Android and Native JS environments
  - It implements modern security and usability best practices for native app authentication and authorization.
  - The library follows the best practices set out in RFC 8252 - OAuth 2.0 for Native Apps
  - WebPage: https://appauth.io/
- Used as a base implementation
  - Popular and well-known solution
  - Follow best practice
  - Open source
  - Backed by google

Android AppAuth Federated extension

- Original Repository: https://github.com/openid/AppAuth-Android
- The AppAuth demo app is extended for offering OIDCFed support
  - Repository: https://github.com/alejandro-perez/AppAuth-Android/tree/federation_rebased
- We provide a generic Java library to generate and process OIDC Federated metadata statements
  - Functions
    - Constructing a Signed Metadata Statement
  - Verifying the Metadata Statement
  - Flattening the Compounded Metadata Statement
- Makes use of Nimbus JOSE + JWT library
  - https://connect2id.com/products/nimbus-jose-jwt
- Not limited to Android, also used in Shibboleth OIDCFed support
- Repository: https://github.com/alejandro-perez/OIDCFederatedMetadataStatement
- **Status: Working POC**

iOS AppAuth Federated extension

- Original Repository: https://github.com/openid/AppAuth-iOS
- The AppAuth Example-iOS_ObjC is extended for offering OIDCFed support
- Extended the AppAuth library to process OIDC Federated metadata statements
  - OIDCFed functions implemented in the OIDFederatedMetadataStatement classes
    - Constructing a Signed Metadata Statement
    - Verifying the Metadata Statement
    - Flattening the Compounded Metadata Statement
    - Additional cryptographic functions to convert from JWK public and private keys to PEM format (Using OpenSSL library)
  - Makes use of JWT Library: https://github.com/yourkarma/JWT
- Repository: https://github.com/elenatorroglosa/AppAuth-iOS/tree/oidcfed
- **Status: (just recently) Working POC, but still a work in progress (cleaning code, debugging the flow control in different cases)**

Elena Torroglosa
emtg@um.es

GÉANT
Networks · Services · People
www.geant.org