MODRNA WG

The interface of MODRNA (Mobile Profile of OpenID Connect) and GSMA Mobile Connect

http://openid.net/wg/mobile/

May 21, 2020

Bjorn Hjelm
Verizon

John Bradley
Yubico
Purpose

- **Support** GSMA technical development of Mobile Connect
- **Enable** Mobile Network Operators (MNOs) to become Identity Providers
- **Developing** (1) a profile of and (2) an extension to OpenID Connect for use by MNOs providing identity services.
What is Mobile Connect

- Mobile phone numbers as user identifier.
- Mobile phone number as authenticator.
- MNO (Mobile Network Operator) as authentication/identity provider.
- Replace passwords and hardware security tokens.
Mobile Connect – How It Works

1. MODRNA Registration Profile – Set up credentials
2. MODRNA Discovery Profile – MNO discovery
3. MODRNA Authentication Profile – Authentication Request
4. MODRNA Authentication Profile – Authentication Request
5. Your customer is authenticated via their mobile
6. Your application or web service
7. Discovery service
8. Your customer on desktop/mobile/tablet

Source: https://developer.mobileconnect.io/about/
Working Group Status

- Completed second Implementer’s Draft of CIBA Core specification.
- Four specifications in Implementer’s Draft status.
  - Authentication Profile, Account Porting, User Questioning API, CIBA Core.
- Currently working on updating three drafts.
  - Discovery Profile, Registration Profile, MODRNA CIBA Profile.
- Starting discussions on OpenID Certification for profile.

More information available at https://openid.net/wg/mobile/status/
MODRNA WG
Collaborations and Outreach
Evolution of **Mobile Connect** architecture, functionality and identity services.

**RCS** (Rich Communications Services) services support for OpenID Connect.

Configuration of device-based services with embedded SIM (ODSA, C-V2X) leveraging OpenID Connect for authentication.
- Mobile Connect Interest Group (MCIG) replaces the previous efforts provided by the GSMA Identity Program.
  - MCIG is a forum for GSMA members to collaborate on matters relating to the operation and commercial growth of Mobile Connect and Identity services.
- The MCIG Technical subgroup (TSG) is responsible for maintaining the MC Product and Core framework specifications.
- Collaboration effort re-established with updates being shared between the organizations and coordination of efforts.
- Proposal for a joint OpenID Foundation – GSMA MCIG workshop being discussed.
3GPP Mission Critical Services

3GPP (Third Generation Partnership Project) Mission Critical (MC) services support PSA (Public Safety Agencies) and other critical communications.

Identity management part of MC system security architecture. OpenID Connect MCX Profile used for user authentication.

Current development of SEAL (Service Enabler Architecture Layer) for Vertical (V2X) services based on MC architecture.
Create the future together.