

Mi-UAP

Unified Authentication Platform

Mi-UAP enables single sign-on (SSO) across multiple applications, and multiple enterprises. It provides multi-factor authentication (MFA) capability; and authentication adaptivity taking into account user action against machine-learned norms, application-specific trust establishment specifications, and environmental context. Mi-UAP allows SSO interactions using mobile applications inclusive of MY Digital Identity (MY-DID).

Overview

Mi-UAP is specifically designed for operational risks arising from user authentication and identity management (IDM). It is an Identity Provider (IDP) realisation of the Security Assertion Markup Language (SAML) framework, enabling SSO to multiple cloud-connected Service Provider (SP) applications. Mi-UAP provides a uniformly high standard for authentication; in addition to enrolment and credential issues from user and system-initiated security cases. Application systems are relieved of the responsibility and risk of user identity and credential management.

Features

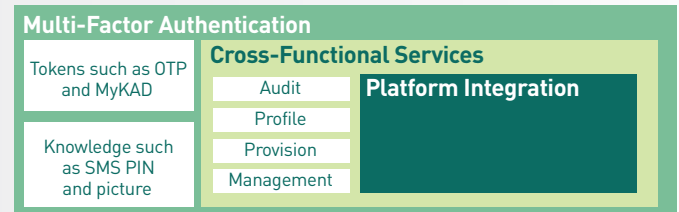
Mi-UAP provides the following features:

- Single Sign-On (SSO)**
 Users are able to use individualised credentials for authentication (who-am-i) into multiple application URL domains and directories. Individual applications are responsible for authorisation (what-can-i-do).
- Multi-Factor Authentication (MFA)**
 Users can establish one or more authentication factors: elliptic curve cryptographic (ECC) protocol, one-time key (OTK) generators (via hardware token or mobile application), public-key infrastructure (PKI) certificate and MY-DID mobile application.
- Adaptive Authentication**
 Service applications can establish trustworthiness requirements based on previous behaviour and environmental factors, where users submit one or more authentication inputs of different trust valuations.
- Authentication as a Service**
 Service providers are able to establish credential consistency, reusability and universality. Application components within the architecture would regulate authorisation.

Technology Benefits

The main impacts of Mi-UAP are:

- Risk Management**
 Users have access to high-security authentication and identity management (IDM) mechanisms, resulting in risk minimisation. This enables a high degree of process integrity, security against man-in-the-middle (MITM) attacks, and (in certain cases) non-repudiation.
- Separation of Concerns**
 Enterprise security assessment is greatly simplified as service applications only need to manage authorisation. De-identified information is accessible to users upon correct demonstration of credential ownership.
- Effectiveness and Scalability**
 User provisioning and enrolment can be undertaken once, and distributed over multiple service applications. Integration requirements, equivalent to SAML compliance, is undertaken for existing and new applications.



Mi-UAP system architecture

Applications

Government, Healthcare, Education, Financial Services

