MIMOS Unified Authentication Platform (Mi-UAP)

The Mi-UAP platform enables single sign on (SSO) across multiple applications, and also multiple enterprises. Mi-UAP provides multi-factor authentication (MFA) capability; and also authentication adaptivity which takes into account user action, variations thereof against machine-learnt statistical norms, application-specific trust establishment specifications, and environmental context. Mi-UAP furthermore allows for SSO interactions to be undertaken using MIMOS-developed mobile applications inclusive of the MY Digital Identity (DID).

Overview

The Mi-UAP platform is specifically designed to operational risks arising from user authentication and identity management (IDM). UAP is an Identity Provider (IDP) realisation of the Security Assertion Markup Language (SAML) framework, enabling SSO to multiple cloud-connected Service Provider (SP) applications. SAML integration is a standard capability in multiple application frameworks, inclusive of Amazon Web Services (AWS); Apache Spring; Microsoft Active Directory (AD), Azure and Office-365; IBM Websphere and Liberty; HP Icewall, Intel Cloud and Redhat Keycloak.

The central value proposition for the UAP platform is provide a uniformly high standard for authentication; in addition to enrolment and credential issue, as might arise from both user and system-initiated security cases, and subsequent management thereof. Application systems are therefore relieved of the responsibility, and therefore risk, of user identity and credential management.

Features

- **Single Sign-On (SSO)**
  Users are able to use individualised credentials for authentication (who-am-i) into multiple application Uniform Resource Locator (URL) domains and directories. Individual applications would therefore be responsible for authorisation (what-can-i-do) within the business context of interest.
- **Multi-Factor Authentication (MFA)**
  Users can establish one or more authentication factors inclusive of password: based on elliptic curve cryptographic (ECC) protocol, one-time keys (OTK) generators (via hardware token or mobile application), public-key infrastructure (PKI) certificate and the MY-DID mobile application.
- **Adaptive Authentication**
  Service applications can establish trustworthiness requirements, which require users to submit one or more authentication inputs, each of different trust valuation. The trust requirement for any particular authentication interaction would also vary based on adherence to statistics derived from previous behaviour, and furthermore environmental factors associated with such interaction.
- **Authentication as a Service**
  Service providers are able to establish credential consistency, reusability and universality. Application components within the encompassing architecture would therefore only need to regulate authorisation.

Technology Benefits

- **Risk Management**
  Users have access to high-security authentication and IDM mechanisms, resulting in risk minimisation. The operational doctrine of flesh-and-blood user specification also enables a high degree of process integrity, security against man-in-the-middle (MITM) attacks, and (in certain cases) non-repudiation. Credential issue and user-to-credential association can furthermore be undertaken at high-assurance levels, with uncompromised protection against administrator negligence or even active misbehaviour.

Technology Summary

Mi-UAP

A SSO platform with high-security characteristics for authentication, enrolment and IDM; as can be integrated into multiple service applications.

Industries: Government, Healthcare, Education, Financial Services

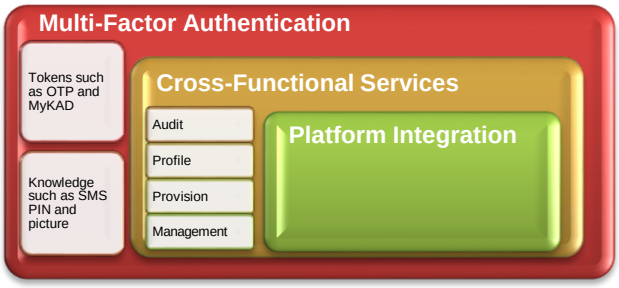
Features

- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Adaptive authentication
- Authentication as a Service

Technology Benefits

- Risk management
- Separation of concerns
- Effectiveness and scalability

- **Separation of Concerns**
  Enterprise security assessment is greatly simplified, due to service applications only needing to management authorisation within the business context. This separation also enables a higher degree of user privacy protection, in that application-side data can be maintained as de-identified information accessible to users only upon correct demonstration of credential ownership.
- **Effectiveness and Scalability**
  User provisioning and enrolment can be undertaken once, and subsequently distributed over multiple service applications. The cost of any UAP deployment are similarly distributed over multiple applications. UAP integration requirements are equivalent to SAML compliance, and is straightforwardly undertaken both for existing as well as new applications.



MIMOS Mi-UAP system architecture

System Requirements

Mi-UAP	
Host Server Requirements	
Processor	Quad-Core
Memory	Minimum 8GB of memory
Disk Storage	Minimum 80GB of hard disk space
Operating System	Ubuntu 12.04 LTS
Virtual Machine Requirements	
Processor	Dual-Core
Memory	Minimum 4GB of memory
Disk Storage	Minimum 10GB of hard disk space
Operating System	Ubuntu® 12.04 LTS

004-0930A