



INFORMATION AND COMMUNICATION TECHNOLOGY SPECIAL INTEREST  
GROUP (ICTSIG)

# DIGITAL ID

BEM Approved CPD/PDP Hours:  
Ref No :

**SPEAKERS:**  
**MR. NG KANG SIONG (MIMOS)**  
**MR. ALWYN GOH (MIMOS)**

**SATURDAY | 17 AUGUST 2020 | 10 AM – 12 PM**

Registration Fees (effective 1st August 2020)

IEM Members : RM 15.00

IEM Non Members : RM 50.00

Register online | [www.iem.org.my](http://www.iem.org.my)

Register Online at [www.iem.org.my](http://www.iem.org.my)

## SYNOPSIS

The Digital ID framework comprises mobile application and server components, respectively associated with individual users and service providers (SP), and enables users to undertake authentication and digital signature computation within the context of a stringent mutual authentication. The Digital ID application is available as a free download on both Android and IOS application stores. Users then undertake identity binding and authenticator establishment via submission of real-world proof-of-identity operations, inclusive of establishment of MYkad ownership by means of fingerprint verification, success of which results in issue of public-key (PK) certificate, with the user name and Identity Card (IC) number integrated therein subject to validation. These user certificates are applicable as common credentials for trust establishment and authentication with any SP server in the Digital ID framework.

Server certificates issued to SP operators likewise enables trust establishment and mutual authentication with any mobile application personalized with a user certificate. This is very different in comparison to common authentication systems, ie as based on password and OTK inputs, which are bound to the issuing SP operator within a closed system. The Digital ID framework, by way of contrast, enables users and business systems; in the tangible form of application-server and browser-server systems; to openly undertake interactions within the context of the protective mutual authentication framework.

The Digital ID framework operates at the highest possible Level of Assurance (LOA) of the ISO 29115 standard for Identity Management (IDM) and Privacy systems. The technical realisation of the necessary security functional requirements towards meeting the specified authentication, assurance and trust objectives is also Common Criteria (CC) certified at the Entity Assurance Level (EAL) of 3+. The signature outcomes of the Digital ID application are furthermore cryptographically non-repudiable, with legal recognition of such signatures by virtue of the Digital Signature Act (1997) and the Electronic Commerce Act (2006).

This presentation is intended to provide engineering insights into the Digital ID framework. We also intend to spark curiosity among IEM members with respect to potential service cases and collaborative work with MIMOS and its partners.

## SPEAKER'S BIODATA



Mr. Ng Kang Siong serves as Principal Researcher at Information Security Lab (ISL) in MIMOS Berhad, a public research organization in Malaysia. He leads a team of researchers and engineers to conduct research and development of information security technologies in addition to providing consultations to key government organizations on application architecture security. He holds a Bachelor of Engineering in Computer and Communication with first class honors from Universiti Sains Malaysia and a Certified Information Systems Security Professional (CISSP) by International Information System Security Certification Consortium (ISC)2.



Mr. Alwyn Goh is an experienced and well-published researcher and engineer in information security, cryptography, biometrics, analytics and medical informatics. He is presently attached to the Information Security Laboratory (ISL) of MIMOS, which is the national research institute for ICT systems. Mr. Alwyn holds the Bachelors in Electrical Engineering and Physics from University of Miami and also a Masters in Theoretical Physics from University of Texas at Austin .

Register Online at [www.iem.org.my](http://www.iem.org.my)