



# Mobile Digital Identity Ecosystem

## Everything you are looking for a trusted digital identity Ecosystem

**Mobile ID** offers a set of multi-layered authentication and identity management services, enabling any MNO to easily become universal digital identity provider.

This course will allow you to easily understand the main standards, stakeholders, technologies, features & security around this **Mobile Digital ID** ecosystem, including **Secure Elements, Authenticated Applications and Solutions** compliant with GSMA Mobile Connect.

**Mobile Digital Identity** requirements for co-operation between these different stakeholders, and **Global Platform** concepts for security and confidentiality will also be explained.

### ■ At the end of the training you will

- > Be able to understand Mobile ID Ecosystem
- > Have an overview on UICC **(SIM) Secure Element** functionalities
- > Know how the **different actors** can **manage several applications on the same card** via Global Platform **(GP)** specifications

### ■ Pre-requisites:

- > No specific pre-requisites for this course  
This course is held in English

### ■ Who should attend?

All people involved in Mobile Identity project:

- > Marketing Managers
- > Project Managers
- > Technical team
- > SIM Manager
- > VAS Manager
- > Operational Team
- > Security Managers
- > ...

## KEY TOPICS

- > GSMA
- > Mobile Connect
- > Secure Elements (eSE,  $\mu$ SD, UICC)
- > ETSI
- > Security Domain / ISD
- > Global Platform 2.2
- > LoA
- > OPEN ID



## DAY 1

### Introduction to Mobile Connect What is Mobile Connect?

- > What is Mobile ID?
- > Use Cases
  - Online Bank Auth
  - Mobile Money Transfer
  - E-government services
  - VPN access
  - SSO & Identity
  - ...
- > Mobile ID users (employees, partners, customers, consumers, citizens)
- > Ecosystem evolution
- > Digital Identity standards (ETSI, OPEN ID Connect)
- > Identity organizations (GSMA, OPEN ID, FIDO)
- > Trust frameworks (OIX)

### Focus on Security

- > Types of attacks
- > Risks involved
- > Consequences for User/Service Provider

- > Basic principles of Securing User identity & online transactions (Identity, Authenticity, confidentiality, non-repudiation)
- > PIN solution (advantages & limitations)
- > Symmetric cryptography solutions (idem)
- > PKI principles
- > Mobile Connect key Authenticators (LoA, Usage & Security)
- > Authentication methods (OTP, Password, PIN, Mobile, PKI, biometrics...)
- > OpenID, SAML

### Focus on Secure Element

- > JavaCard-based SIM Cards
  - Introduction
  - Architecture
  - Applet management
  - INSTALL(Load), LOAD, INSTALL(Install) Commands
- > STK and JavaCard-based SIM Card
  - STK reminder
  - Event management
  - Toolkit Installation parameters
  - Proactive commands structure

## DAY 2

### Global Platform Basics

- > What is GlobalPlatform?
- > How actors can manage their applications on the same card
- > What is a Security Domain & how can it be used?
  - Privileges, market trends...
- > Secure Channel Protocol
- > Card Content Management basics (INSTALL, LOAD, PERSO, EXTRADITION...)
- > Global Platform Commands summary
- > GP Access Control
  - Mechanism to access applications installed in the secure elements

### Focus on Solutions for Mobile Identity Security

- > Market solutions overview
- > Comparison of benefits & limitations of different solutions
- > Best Practices for Deployment via Case Studies
  - Technical & Business considerations
- > Architecture of mobile PKI end-to-end solution
- > Role of each brick in the solution & interfaces with existing infrastructure
- > Actors: who is responsible for what
- > Mobile Network operators: Role & opportunities
- > ETSI 102 204 standard overview and how it is actually implemented in real deployments
- > Demos