GlobalPlatform for NFC

The essentials for managing NFC Services on the Secure Element, shared between MNOs, banks & service providers

Mobile NFC requires co-operation between different stakeholders, each with their own culture and expectations. The overall requirements are: - the need to easily design, deploy & operate services with security and confidentiality.

GlobalPlatform 2.2 is the interoperable standard to allow a secure implementation & communication between parties.

This training will help you to better understand the Global Platform specifications for NFC, including GP2.2 specifications for configuring Secure Element, the amendments A, B, C….for contactless parameters & confidential SE content remote management.

At the end of the training you will:

- Understand the GlobalPlatform 2.2 Smart Card Spec functionalities
- Understand how the different actors (Mobile Operator, MVNO, Bank, and Transport Operator) can share the same Secure Element (SE).
- Understand how to access a GP SE and its applications ‘Remotely’
- Have a technical understanding of the Global Platform 2.2 standards (UICC configuration, Amendment A…)

Who should attend?
All people involved in Mobile NFC project:
- Secure Element Architects,
- Developers
- Product dev team
- Technical team
- Operational Team
- Security Managers

Pre-requisites:
- This course requires participants to have basic knowledge on NFC Ecosystem

This course is held in English
## PROGRAM

### Mobile NFC Ecosystem - Introduction
- Mobile NFC Use Cases
- Overall Solution Architecture & Real deployment examples
- Mobile NFC, User interface, Secure Elements (SE) – Focus on UICC
- Global Platform & Mobile NFC – Different TSM Server and SE architectures

### Global Platform 2.2
- Context & Needs
- Multi-application card and security architecture
- GlobalPlatform Commands (Java Card Application management for NFC)
- Security Domain, privileges and commands
- Business models (simple, AM, DM)
- SCP02, OTA and HTTPs security, and Key management
  - Brief overview of Amendment D (SCP03)
- Differences between GP2.1 & GP2.2

### Global Platform Access Control
- Overview of mechanism & rules applied to mobile applications access to Secure Element applets

### UICC config
- Definition of the minimal GP configuration for a Telecom Secure Element
- Demos:
  - GP hierarchy definition, starting from business requirements + demo

### Card Compliance Program
- Compliance program and how to obtain GP certification
- Demos:
  - Use GP commands
  - Load, install applet
  - Test delegated management

### Amendment A
- Confidential Card Content Management (CCCM), confidential initialization of the 1st service provider keyset

### Amendment B (if required)
- RAM over HTTP management, SCP81, Admin. agent and HTTP session flowcharts

### Amendment C
- CRS, CREL definition, contactless parameters, privileges, Cumulative Granted Memory.