

## Global Platform 2.2

The essential standard for a reliable & interoperable communication between MNO, bank & service providers



Mobile contactless requires trusted **co-operation** between mobile operators, banks, transport companies and other service providers.

The multi-player and multi-application nature makes it essential to provide **high levels of security** and **trust** between parties.

**Global Platform 2.2** is today the only **interoperable** standard to allow a secure communication between these parties.



### At the end of the training you will

- > Understand the Global Platform 2.2 Smart Card Spec functionalities
- > Understand how the different actors (Mobile Operator, MVNO, Bank, and Transport Operator) can share the same card.
- > Understand how to access a GP card and its applications 'Over The Air'
- > Have a overview of the Global Platform 2.2 standards (UICC configuration, Amendment A...)

### Who should attend

- > Bank, Telecom, Transport staff:
- > Service providers
- > Project Managers
- > Security Managers
- > SIM managers
- > System developers

#### Pre-requisites:

- > This course requires participants to have technical knowledge on smart cards or on payment system applications.

This course is held in English

### Key topics

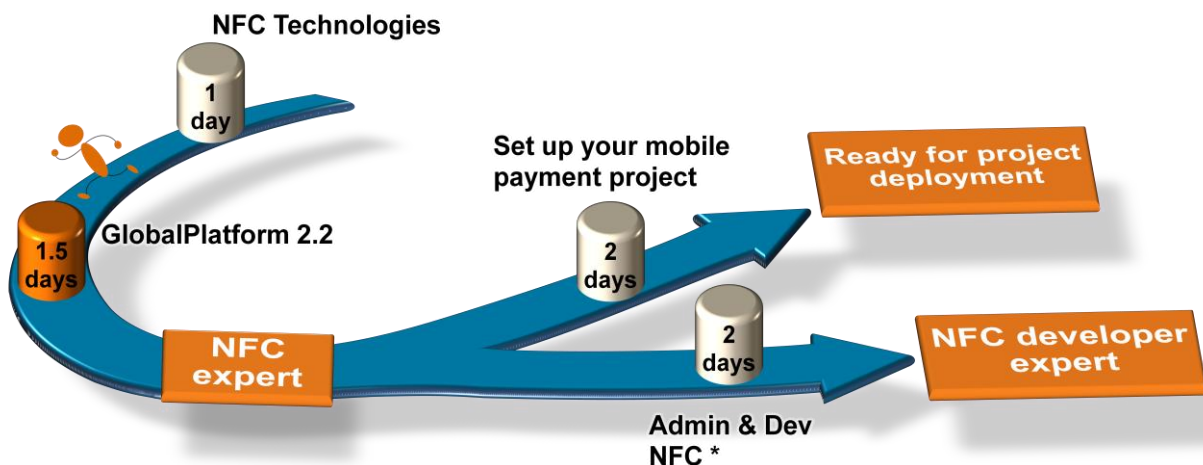
- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>&gt; Multiapplication Card</li> <li>&gt; OTA "Over The Air"</li> <li>&gt; SCP</li> <li>&gt; Security Domain / ISD</li> </ul> | <ul style="list-style-type: none"> <li>&gt; Delegated management</li> <li>&gt; DAP verification</li> <li>&gt; Mandated DAP verification, TSM</li> <li>&gt; Confidential Card Content management</li> </ul> |
|---|--|

# Course Schedule



Day 1	Practice
<p><b>Optionally, overview of a Telecom Card</b></p> <ul style="list-style-type: none"> <li>&gt; Architecture of a telecom card</li> <li>&gt; File system, commands, access conditions &amp; pin system</li> <li>&gt; SMS Header &amp; Security</li> <li>&gt; Remote applet &amp; file management</li> </ul> <p><b>Global Platform 2.2</b></p> <ul style="list-style-type: none"> <li>&gt; Introduction and standard history</li> <li>&gt; Actors and Business cases (Controlling authority, Application Provider, Issuer)</li> <li>&gt; Card and security architecture</li> <li>&gt; GP commands                             <ul style="list-style-type: none"> <li>o Logical channels</li> <li>o Load, install of an applet (ELF, EM)</li> <li>o Commands for cards an applet lyfe cycle</li> </ul> </li> <li>&gt; Security Domains &amp; applet privileges</li> <li>&gt; SD Privileges: Card Content Management                             <ul style="list-style-type: none"> <li>o Delegated management</li> <li>o DAP verification</li> <li>o Mandated DAP verification</li> </ul> </li> <li>&gt; Privileges for services</li> </ul>	<p>Use GP commands</p> <p>Load, install applet</p> <p>Test delegated management</p>

Day 1.5	Practice
<p><b>Global Platform 2.2</b></p> <ul style="list-style-type: none"> <li>&gt; Confidential Card Content Management” Amendment A of in GP 2.2                             <ul style="list-style-type: none"> <li>o OTA Security domain creation with Key allocation (OBKG, temporary keys)</li> <li>o Confidential Application loading</li> <li>o OTA Confidential personalization</li> </ul> </li> <li>&gt; Key management</li> <li>&gt; Secure Channel Protocols SCP 02 80 10</li> <li>&gt; “UICC Configuration”</li> </ul>	



\* Pre-requisites: (U)SIM basics, Dev STK