Understanding Trusted Execution Environment (TEE)

Everything you need to know about TEE for deploying secure mobile services

Convenient & user-friendly mobile device services & applications are hugely deployed. Thanks to the enhanced security offered by the Trusted Execution Environment many additional opportunities are open to service providers.

This course will allow you to easily understand the main standards, technologies, features & security around this ecosystem

At the end of the training you will

> Understand the main concepts, use-cases & standards for Trusted Execution Environment (TEE);
> Be able to describe the main security features of TEE;
> Understand TEE's functional architecture & APIs for interfacing;
> Have a clear overview on TEE implementation based on a real example, including a demo;
> Understand how TEE solutions can be combined with Secure Elements;
> Be able to describe how TEE life cycle may be remotely managed with Trusted Service Management (TSM) solution

Who should attend?

All people involved in Mobile Services project:
> Marketing Managers
> Project Managers
> Technical team
> VAS Manager
> Operational Team
> Security Managers
> …

Pre-requisites:
> No specific pre-requisites for this course

This course is held in English

Key topics

> TEE
> HW-SW Architecture (REE/TEE)
> Security Features
> APIs
> SE & TEE
> TSM for TEE
**Course Schedule**

### Day 1

**Introduction to Trusted Execution Environment (TEE) & Standards**
- TEE overview
  - Concepts & History
  - Ecosystem
  - Solutions & Use Cases
- GlobalPlatform (GP) standards

**Security Essentials of TEE**
- Global TEE Architecture
  - HW/SW separation of REE/TEE
  - Secure boot
- Intrinsic TEE security features
  - Trusted Zone,
  - Memory/process isolation, ...
- Security evaluation and certification
  - GlobalPlatform, Common Criteria

**Functional Architecture & Interfaces**
- System Architecture overview
- Services and APIs
  - Client API
  - Internal Core API
  - Trusted User Interface
  - Remote Administration
  - SE Access API
  - Socket API
  - Debug API

**TEE combined with Secure Elements (SE)**
Coupling SE and TEE (main models, secure channels…)

**TSM for TEE Ecosystem**

**TEE Use Case Demonstration**
- Use Case overview
  - Features and Design
  - Workflow
- Live demo