Java Tee
Java Trusted Execution Environment Emulator

Motivation
The Trusted Execution Environment is a standardized processing environment for sensitive data. The TEE specifies a number of basic components for communication, cryptography, data storage etc. for a C runtime environment. It is great for developing small footprint Trusted Applications, but it lacks the comfort and flexibility of a managed runtime such as Java, which hampers rapid prototyping of fresh new ideas. This is where you come in!

Project Description
Goals
• Understand Security by Isolation
• Implement a runtime for Trusted Applications

Background
• Basic Java
• No other prior knowledge required, interest in Security by Isolation
  • GlobalPlatform Device Technology TEE API Specifications

Deliverables
• A TEE emulator implementation in Java
• Documentation/Tech Report
• Presentation (15 -20 Minutes)

Scope and Credits
Studies:  ☑ INF  ☑ SEW  ☑ TEL  ☑ MATH
The scope, effort, and credits of this project are scalable

Advisor/Contact
daniel.hein@iaik.tugraz.at
johannes.winter@iaik.tugraz.at

Graz University of Technology
Institute for Applied Information
Processing and Communications
http://www.iaik.tugraz.at/