The main goal of the project is to set up a mockup of secure device running a Trusted Execution Environment. A TEE is a hardware and software solution aimed to add security to a microprocessor or a SOC. This can be achieved by adding an external dedicated secure processor like a secure element or a SIM card; another approach consists of creating a “secure enclave” directly into the microprocessor. The concepts of TrustZone (ARM) or SGX (INTEL) are following this second approach. A TEE has always CPU and memory resources and it’s designed to run Trusted Application (TA).

**Principle:**

The microprocessor (or the electronic board) is separated into two different areas

- A “Normal world” is used to run a high level OS with application(s) in interaction with users, networks, and servers (like Linux, Android…). This is the REE.
- A “Secure world” is used to run a small and secure code. It can be either a dedicated application or a small OS plus one trusted application offering different kind of services to the normal world.

Typical use cases: mobile payment and financial services (NFC, account number, assets or credentials) in smart phones, cryptographic keys and digital rights management, and secure firmware update. This is also a proposal to add security to the world of IoT.

Typical hardware using this solution: smart phone, POS terminal, secures devices.

The hardware target for this internship is an evaluation board equipped with an ARM M35P (preferred) or M33 processor including a TrustZone © IP and additional security material like hardware PUF.

**Project steps and deliverables**

1. State of the art of TEE solutions
2. Development of a fully operational mockup. Expected functionalities are:
   - A rich execution environment (REE) running on the Normal world, with a full functionalities Operating System like Linux or Android OS ;
   - A Secure world using TZMA, TZPC, TZASC and running a TEE OS ;
   - A couple of applications (App on REE + Trusted App on TEE) used for the demonstration of different kind of services
     - a secure and trusted boot mechanism using PUF technology ;
     - a service for keys provisioning from a server, using PUF for authentication and security ;

**Project Keywords**

ARM, TrustZone, Secure Boot, assets management, electronic board, GlobalPlatform, Rich Execution Environment (REE), Trusted Execution Environment (TEE), Physical Unclonable Function (PUF), TrustZone Memory Adapter (TZMA), TrustZone Address Space Controler (TZASC), PKI

**References**

- Trusted_execution_environment
- ARM Trustzone
- ARM Platform-security-architecture
- GlobalPlatform
- Android/security
- SRAM PUF
2. Miguel Guerra, Benjamin Taubmann, Hans Reiser, Silesi Demesie Yalew, Miguel Correira, 2018, introspection for ARM TrustZone with ITZ library

Context:

LCIS laboratory is a part of the Grenoble INP institute and University Grenoble Alps. It’s focused on embedded systems, hardware and software security and safety, RFID and complex system modeling. ([http://lcis.grenoble-inp.fr/](http://lcis.grenoble-inp.fr/))

Chaire Trust is a program launched by the Foundation Grenoble INP and industrial partners. The main objective is to develop skills and new technologies for the security and safety of embedded systems. ([https://fondation-grenoble-inp.fr/nos-actions/contribuer-developpement-recherche/chaire-trust/](https://fondation-grenoble-inp.fr/nos-actions/contribuer-developpement-recherche/chaire-trust/)).

The Grenoble Alpes Cybersecurity Institute – in short, Cyber@Alps – is a project selected in 2017 by the Cross-Disciplinary Program (CDP) of the IDEX Univ. Grenoble Alpes and aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy protection challenges. Our main technical focus are on cost effective secure elements, security of critical infrastructures all along their life cycle, vulnerability analysis and global challenges in terms of risk analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad ([https://cybersecurity.univ-grenoble-alpes.fr](https://cybersecurity.univ-grenoble-alpes.fr))

**Prerequisites**

Applicants must be enrolled in a Master in embedded system or electronics engineering degree.

Skills: C/C++ programming, embedded system, ARM, security and cryptography.

<table>
<thead>
<tr>
<th>Tutors</th>
<th>Laurent Pion, David Hély</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Please send your resume, application letter with recommendations, master's degree grades to <a href="mailto:David.hely@lcis.grenoble-inp.fr">David.hely@lcis.grenoble-inp.fr</a>; <a href="mailto:Laurent.pion@esisar.grenoble-inp.fr">Laurent.pion@esisar.grenoble-inp.fr</a>;</td>
</tr>
<tr>
<td>Location</td>
<td>The student will be hosted at the LCIS laboratory in Valence (Drôme), France</td>
</tr>
<tr>
<td>Starting date</td>
<td>February 2020</td>
</tr>
<tr>
<td>Duration</td>
<td>The position is 5 months long</td>
</tr>
<tr>
<td>Allowance</td>
<td>The gratification is in accordance with existing regulations, approximatively 560€/month.</td>
</tr>
</tbody>
</table>