# Convert this docx to PDF before submitting it to Collab No code submission needed

# TEE Q&A (10 pts each)

Answer each question in **a few sentences**.

1. Why do we need TEE, given that the OS kernel is already providing isolation and protection to applications? State the security advantage of TEE vs. OS. What security protection that the TEE can provide but the OS cannot provide.
2. By design, what type of code should execute in TEE? State the design consideration: code size, programming languages, dependencies on 3rd party libraries, execution time, the level of trustworthiness, etc.
3. There is an argument that TEE is more trustworthy than a commodity OS kernel, e.g. Linux. Do you agree? Why? State to which attacks or threats the OS kernel is vulnerable, and to which attacks the TEE is vulnerable. Compare these attacks.
4. What does trusted computing base (TCB) mean? What is the TCB of your smartphone?
5. What is the role of "TEE supplicant"? What does it do?

# Environment setup

Follow the tutorial and run the "helloworld" example

https://fxlin.github.io/p3-tee/quickstart/

1. Are you using QEMU or the Rpi3 hardware? If QEMU, are you using granger1, granger2, your local Linux, your local WSL, or others? (10 pts)
2. Show a screenshot of you successfully running helloworld . It must be generated by yourself (40 pts)