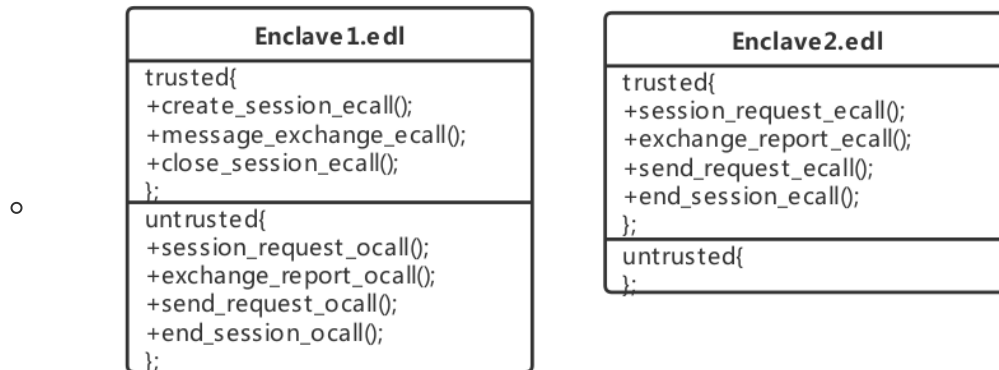SGX学习一周总结

本周已完成任务

- Local attestation

  -

- message exchange

Local Attestation总结

process

1. create Encalve1 and Enclave2

2. create session (Diffie-Hellman Key Exchange)

   1. Enclave1 send a session request to Enclave2 (Session Request)

      1. sgx_dh_init_session();
      2. session_request_ocall();

   2. Enclave2 process request and send msg1 to Enclave1

      1. sgx_dh_init_session();
      2. sgx_dh_responder_gen_msg1();
      3. return msg3;

   3. Enclave1 process msg1 and send msg2 to Enclave2 (Exchange Report)

      1. sgx_dh_initiator_proc_msg1();
      2. exchange_report_ocall();

   4. Enclave2 process msg2 and send msg3 to Enclave2

      1. sgx_dh_responder_gen_msg2();
      2. return msg3;

   5. Enclave1 process msg3 and the session created

      1. sgx_dh_initiator_proc_msg3();

3. message exchange

   1. Enclave1 send message exchange request to Enclave2

      1. send_request_ecall();
      2. sgx_rijndael128GCM_decrypt();

   2. Enclave2 send response to Enclave1

      1. generate_response_ecall();

2. sgx_rijndael128GCM_decrypt();
    4. close session
        1. Enclave1 send close session request
            1. end_session_ocall();
        2. Enclave2 close session and return
            1. end_session_ecall();
        3. Enclave1 close session
            1. close_session_ecall();
    5. destroy Enclave1 and Enclave2

下周计划任务

- 申请EPID？
- 实现remote attestation
- 实现enclave在硬盘上的load和read