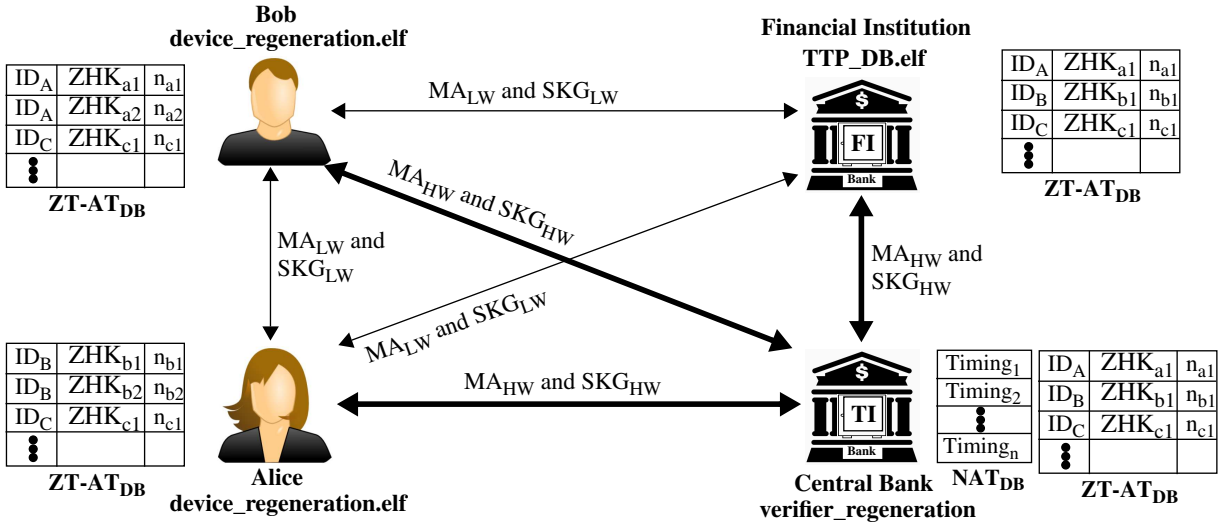
LAB Assignment #8 for ECE 525

Description: ZeroTrust Light-Weight Authentication with FI (TTP_DB.elf)

The overall setup for PUF-Cash is shown in the following figure:

FI: Financial Institution	AT: Authentication Token	MA_{LW}: Light-weight Mutual Authentication
TI: Token Issuer (Central Bank)	HW: Heavy-weight (Timing DB)	SKG_{LW}: Light-weight Session Key Generation
	LW: Light-weight (AT-based)	MA_{HW}: Heavy-weight Mutual Authentication
		SKG_{HW}: Heavy-weight Session Key Generation



In previous labs, we ran code that carried out heavy-weight (HW) authentication, which utilizes the timing databases stored at the Central Bank (also called the TI or token issuer), and light-weight authentication (LW) between Alice and Bob.

In this lab, we add the FI, and light-weight authentication between Alice or Bob and the financial institution (FI). The FI is also a device that possesses an instance of the SiRF PUF.

The FI maintains accounts for Alice and Bob, is multi-threaded and services requests from Alice and Bob for withdrawals and deposits.

The following describes the sequence of operations that occurs in TTP_DB.elf, which the FI runs on the FPGA.

- Open socket to Bank and keep it open permanently.

- GenLLK(): Generate a long-lived key (LLK) with the TI, which the FI will use to generate AT.

  if LLK exists
    Regenerate LLK with SiRF
  else
    MA_{HW}, SKG_{HW} with TI
    Get Chlng
    Generate LLK with SiRF
    Store Chlng info to LLK Table on device

PUF-Cash DB
LLK Table

ID	AID	mask	Chlng	status

ID: chip #
AID: anonymous chip #
mask: Components of Chlng
Chlng: vectors, params, etc
status: 0: un-used, 1: used

- Request TTP-AUTHENTICATION with TI, do MA_{HW}, SKG_{HW}

- ZeroTrustGetCustomerATs()

  if AT do NOT exist
    ZeroTrust_Enroll()

  ZeroTrust_Enroll()
    If LLK non-null, ERROR
    Get number of AT to generate from TI
    For each AT
      Generate nonce, n_x
      CH_LLK = hash(LLK XOR n_x)
      encrypt(CH_LLK) and send to TI
      encrypt(n_x) and send to TI
      TI adds to ZeroTrustAuthenToken table

AuthenticationToken DB
ZeroTrustAuthenToken Table

ID	CH_LLK	n_x	status

ID: chip #
AID: anonymous chip #
CH_LLK: hash(LLK XOR n_x)
n_x: nonce
status: 0: un-used, 1: used

- GetClient_IPs()

  Get TTP IP from TI
  Confirm that TI has same TTP IP

- GetCustomerChipNums()

  TI sends encrypted chip_nums (IDs) for all customers
  FI decrypts list of chip_nums
  FI create an account record for each customer
  FI deposits $100 in each account

PUF-Cash DB
PUF-Cash_Account Table

ID	TID	Amount

ID: chip #
TID: transaction id
Deposit amount

- Create 20 threads and service requests from Alice and Bob
  ALICE-WITHDRAWAL