Bank of America Encryption plan

Project plan:

Aim:

“Data security is fundamental. All new and existing business and data processes should include a data security review. This ensures MIT data is safe from loss and secured against unauthorized access.”

Important Things:

- ✔ *1. Know your Data*
- ✔ *2.Plan Ahead*
- ✔ *3.Scale down*
- ✔ *4. lock it up and back it up*

Know your data:

“Know what data you have and what levels of protection are required to keep the data both confidential and safe from loss. “

Plan ahead:

“*Develop a plan to review your data security status and policies. Create routine processes to access, handle, and store the data safely. Archive unneeded data.”*

Scale down:

Keep only the data you need for routine current business. Safely archive or destroy older data and remove it from all computers and other devices.

Lock it up and back it up!:

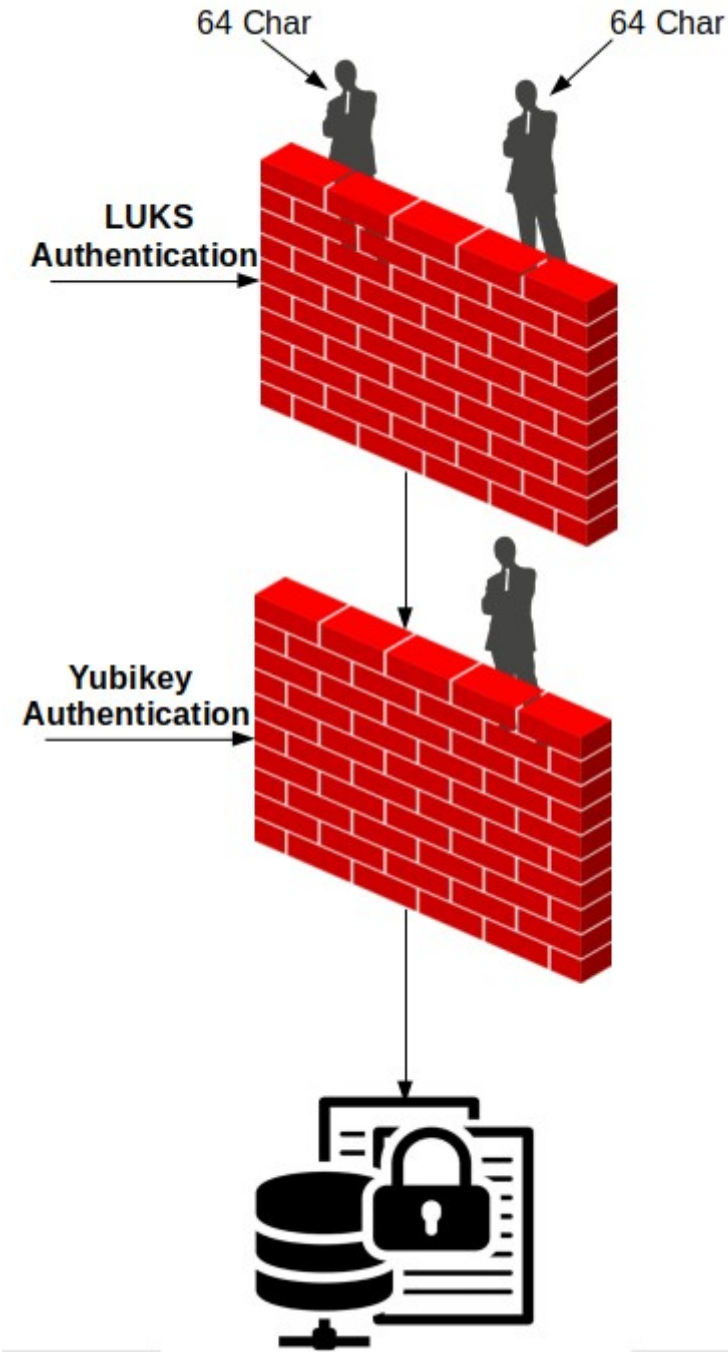
“Physical security is the key to safe and confidential computing. All the passwords in the world won't get your server back if it's stolen.

Backup data to a safe place so it can be recovered if equipment fails or is lost or stolen.

Process Flow:

We have planed to protect our data into two way authenticate encryptyion to decrypt.

- 1. Luks Authentication
- 2. Yubikey Authentication



<u>LUKS-Primary authentication</u>:

To encrypt the server we are using LUKS authentication and in order to access this we need 128 char to finish first level of authentication.

This 128 char is splitted into 2 segments and first 64 segments is handled by Linux Admin and the second 64 segments is handled by Security Admin

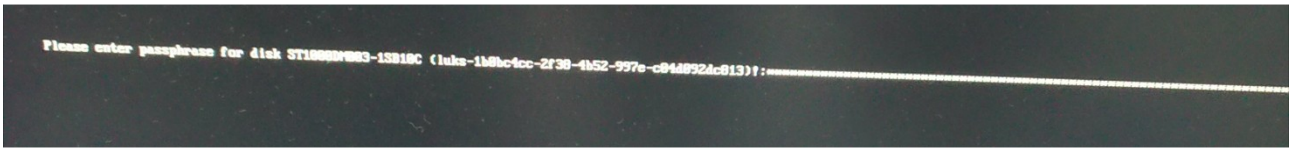
<u>YUBIKEY- Secondary authentication:</u>

This YUBIKEY will be kept and handled by MANAGER LEVEL authority. We need to finish the YUBIKEY level of authentication to enable server login.

<u>PROCEDURES TO FOLLOW:</u>

1. Once LUKS is installed it will be asking for LUKS password in order to Login as it encrypts entire block devices and is therefore well-suited for protecting the contents of mobile devices such as removable storage media or laptop disk drives. The underlying contents of the encrypted block device are arbitrary. This makes it useful for encrypting swap devices. This can also be useful with certain databases that use specially formatted block devices for data storage.

Evidence:



2. The below image represents the after logging in to LUKS and Waiting for Yubikey Access.

Evidence: