Smart Card: SSH Authentication Tool
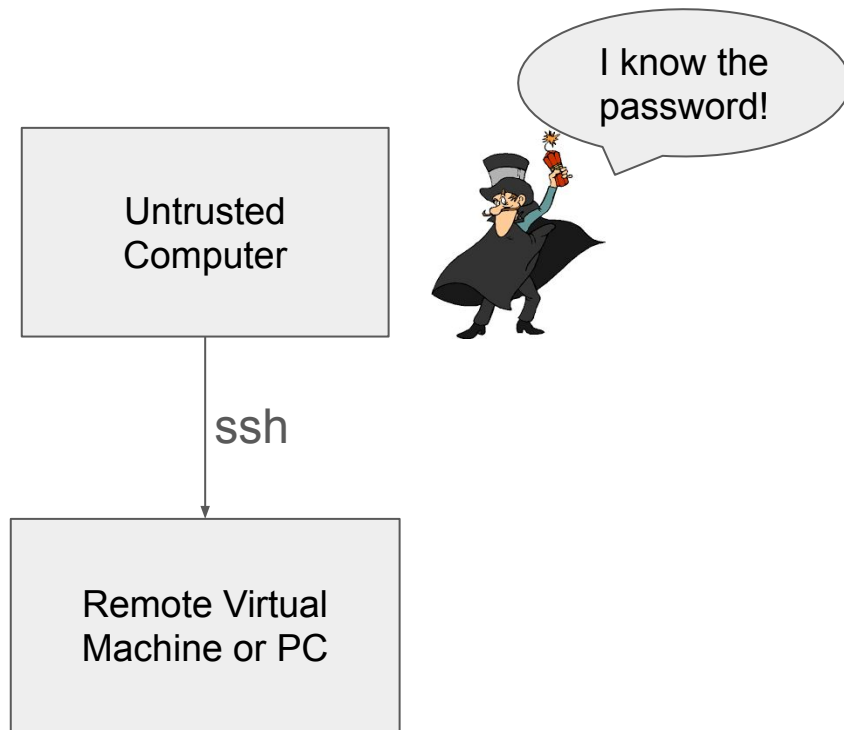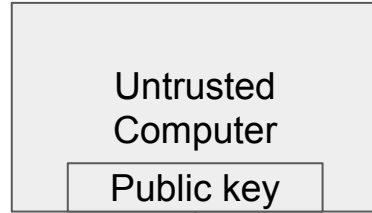
By Qusai Elwazir
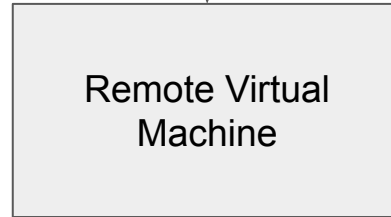
Problem:

Token Based Access

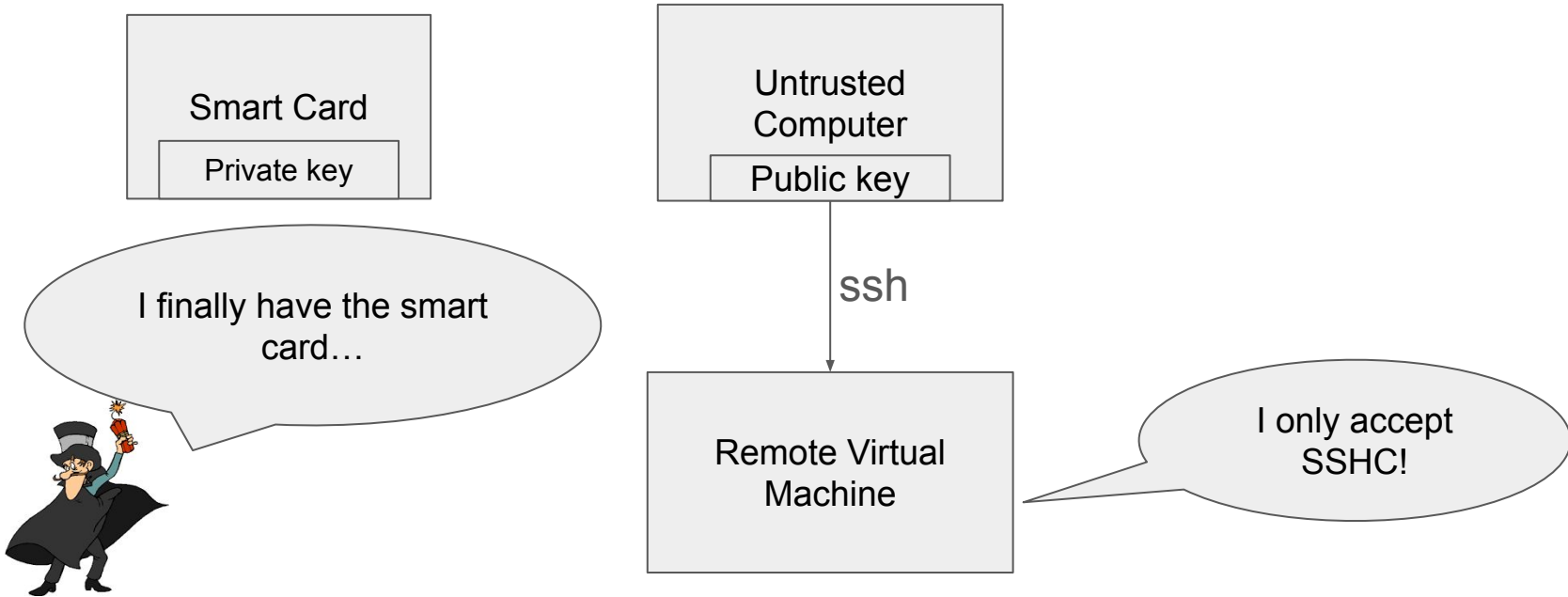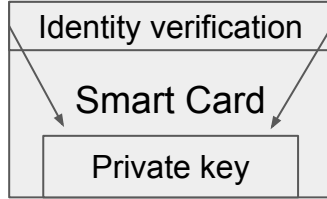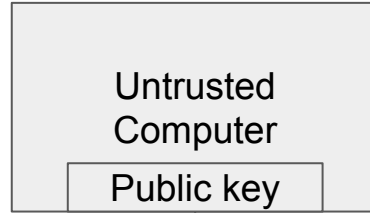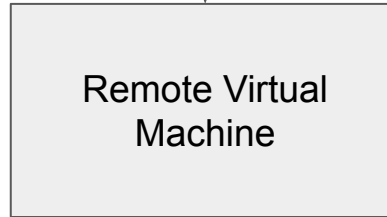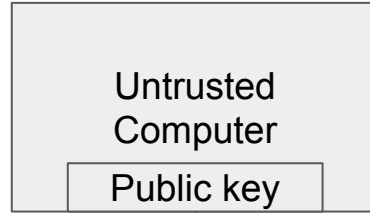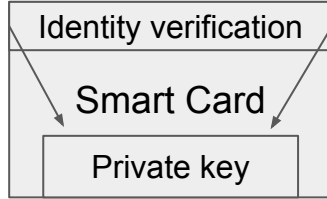# Token Based Access

Token Based Access

Token Based Access

Token Based Access
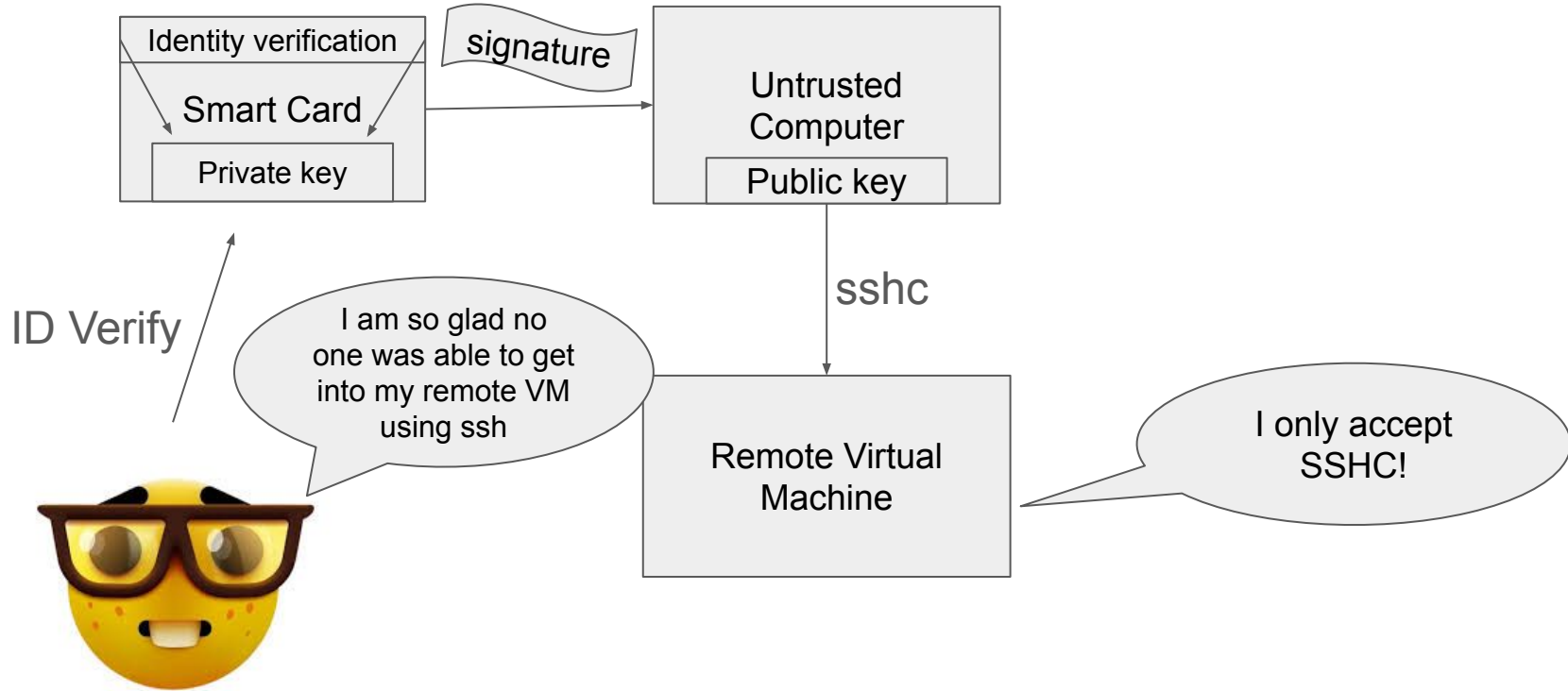
Implementation
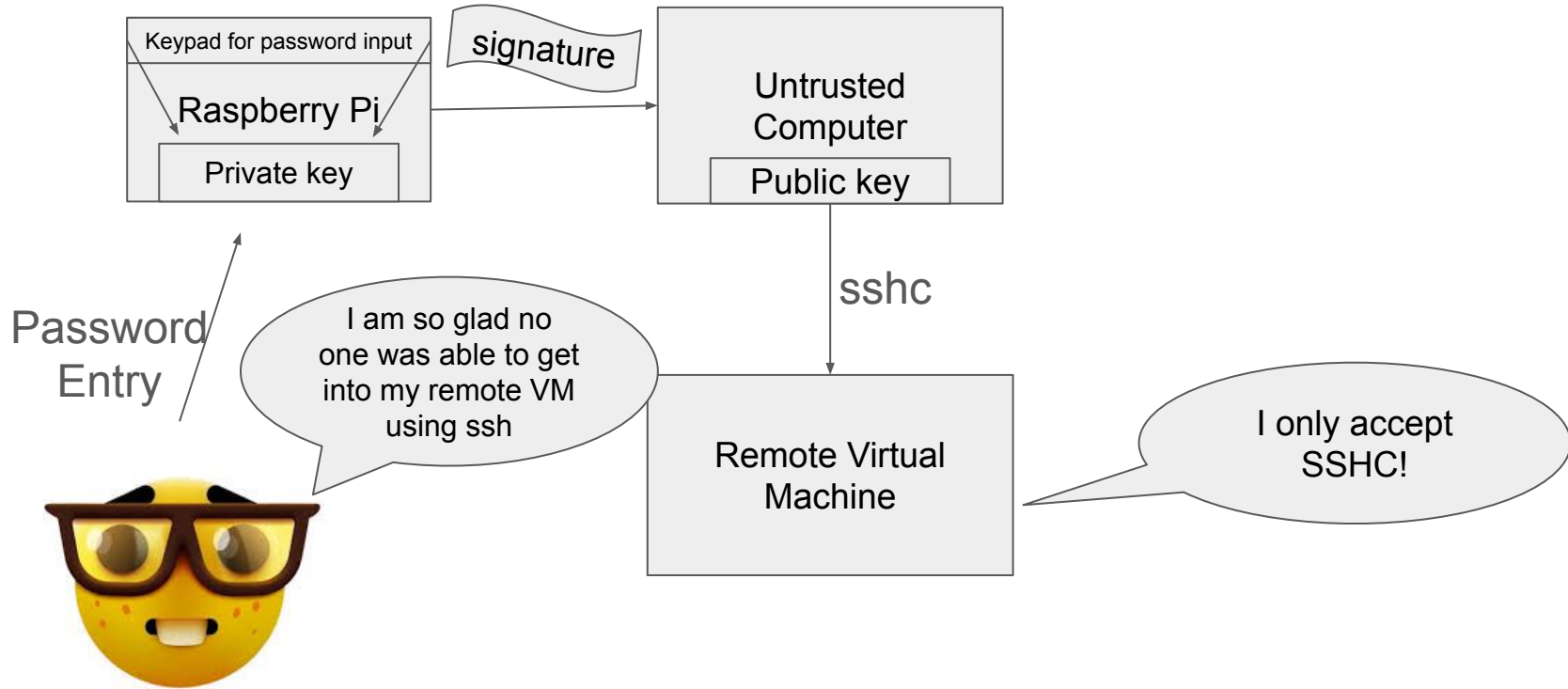
Procedure

1. User invokes sshc module with user ID
2. Machine looks for signature to verify with public key and prompts user to verify identity on the smart card
3. User enters secret code on smart card
4. Smart card creates signature and sends to machine.
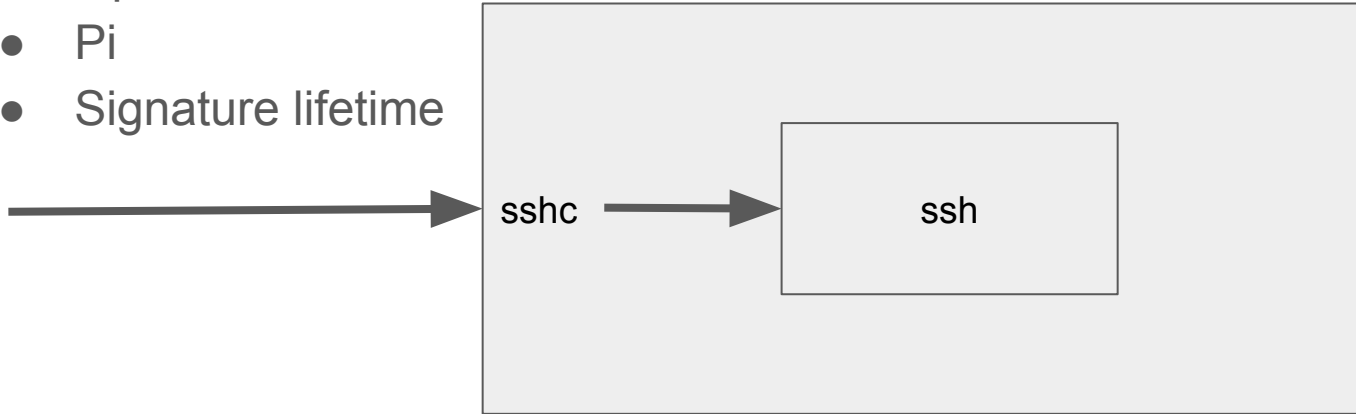5. Machine verifies with public key and signature instance is blacklisted
   a. If not verified return failure
6. Allow ssh into vm

Implementation / implementation Struggles

- SSH-key
- Openssl
- Pi
- Signature lifetime

DEMO VIDEO!

Further development ideas

- module security other than ssh
- More sophisticated signature transmission
- More sophisticated Card identification system
- Streamlined physical design
- Continuous authentication
- Only accept sshc on remote vm

Questions!