

Authentication

UT CS361S

FALL 2020

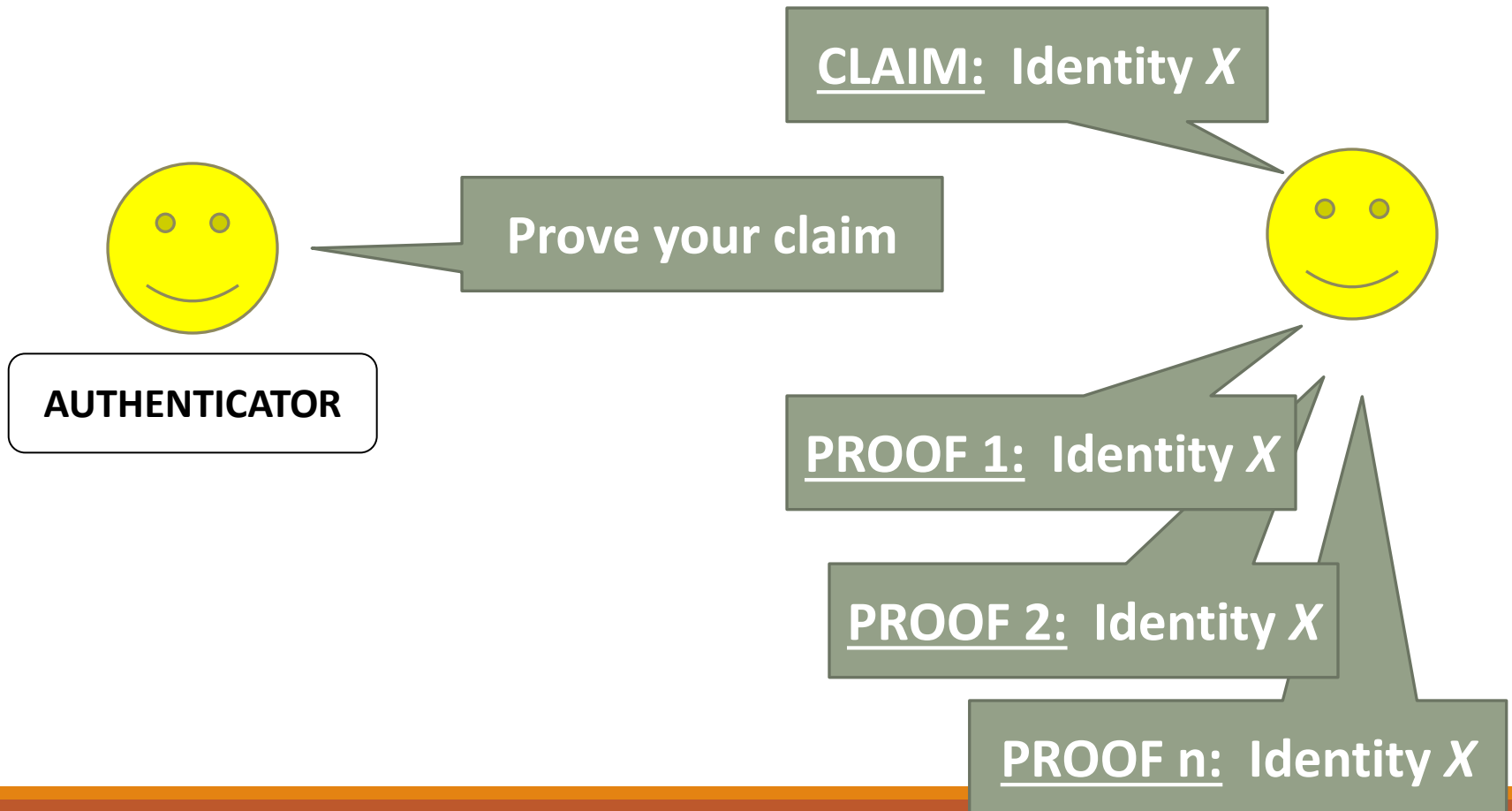
LECTURE NOTES

Authentication/Authorization

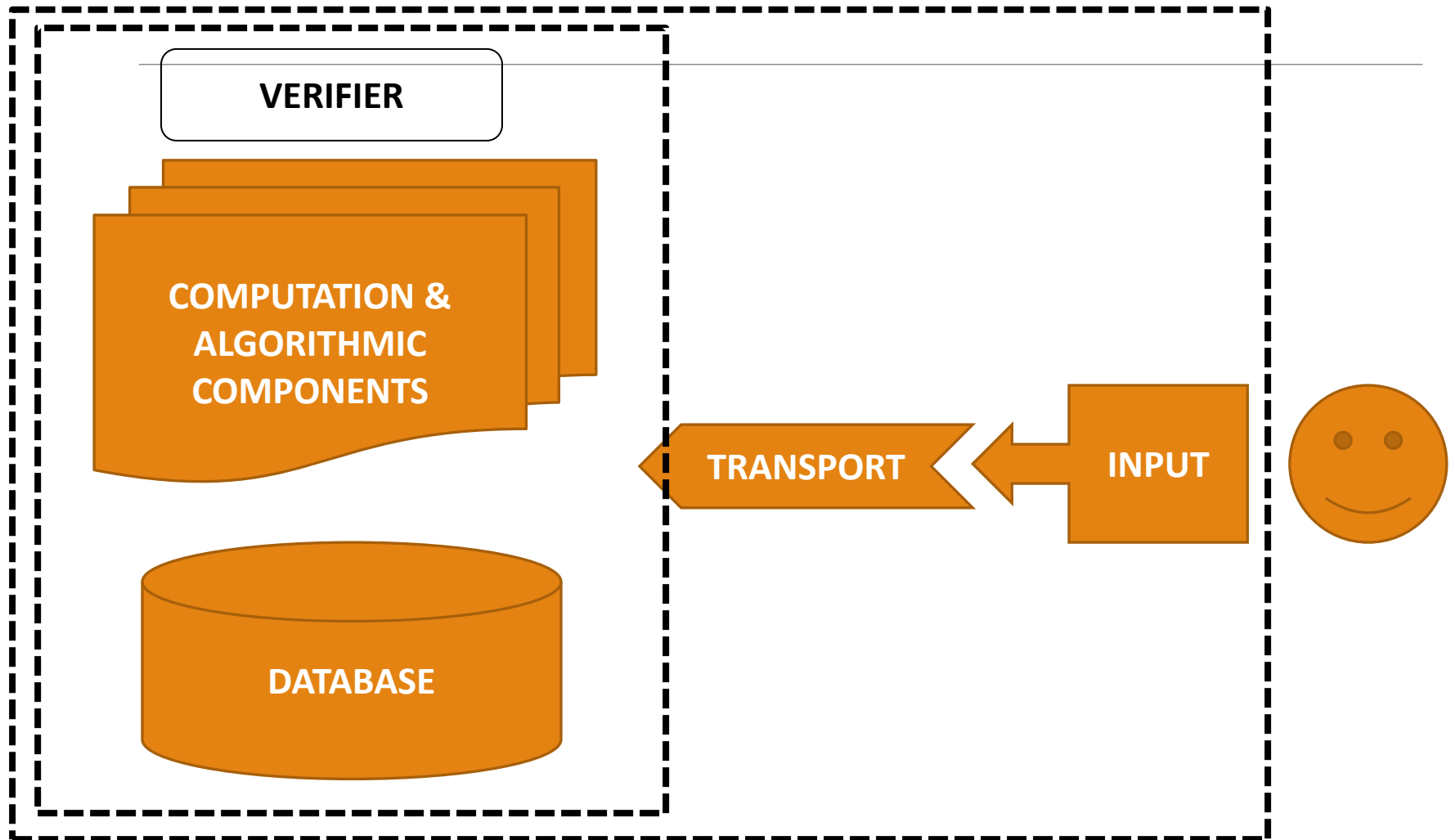
Validating
Identity

Permissions
Assigned to a
Validated Identity

The Authentication Process



Authentication Mechanism



The Big Three

Something you KNOW

Something you HAVE

Something you ARE

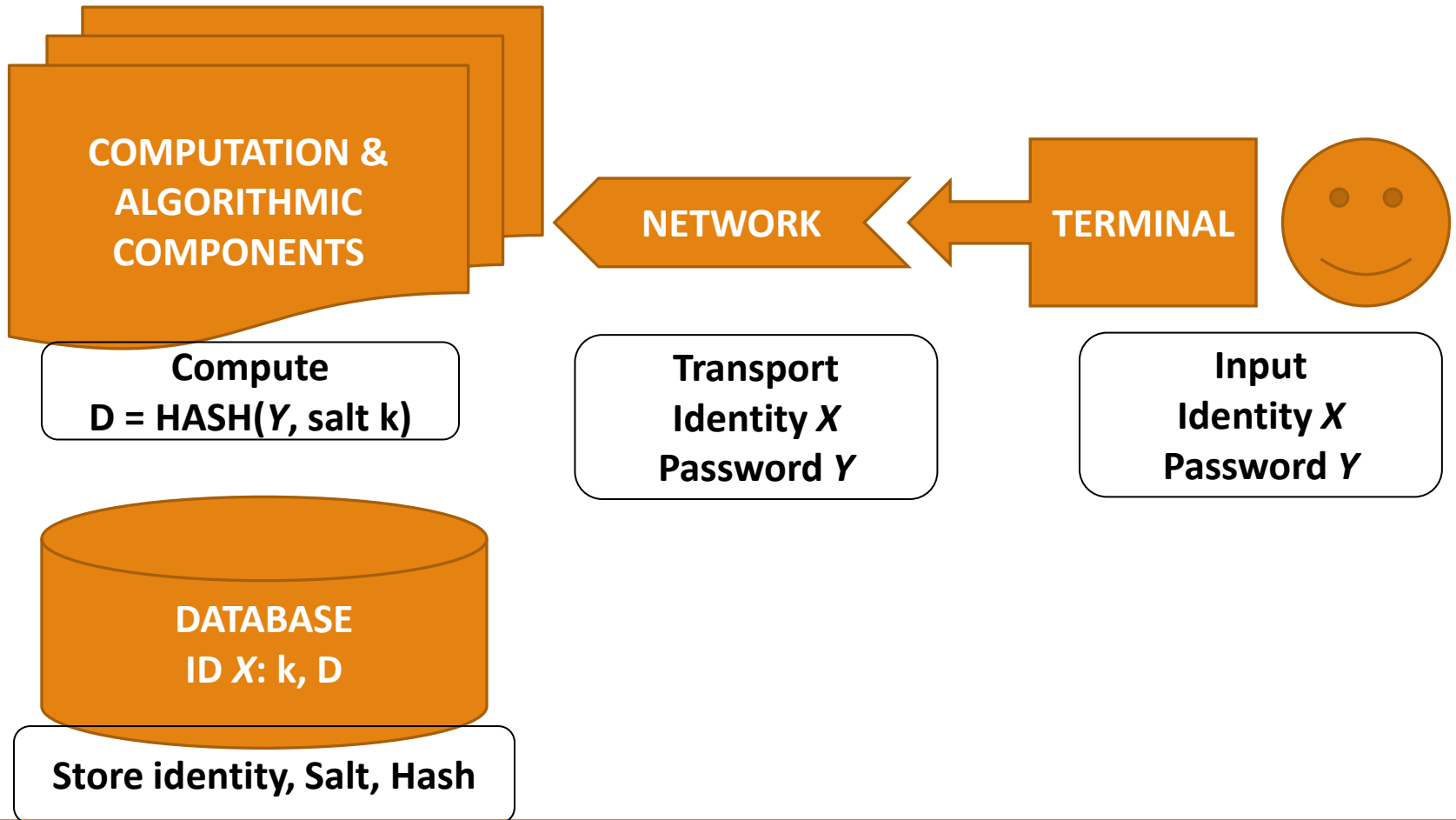


KNOW: Passwords

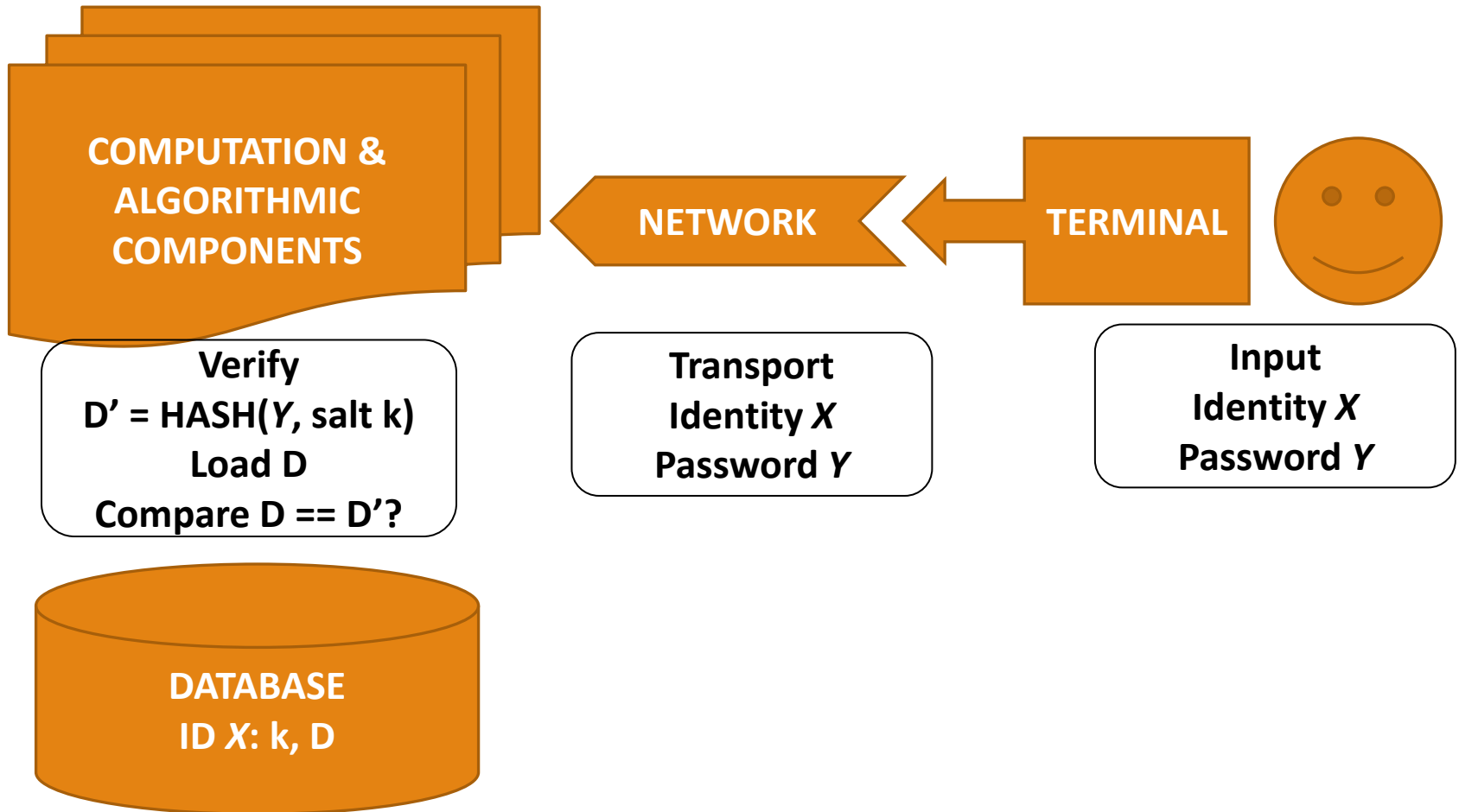
Security Requirements

1. The password is **ONLY** known by the party seeking authentication
2. The password cannot be easily guessed by human or computer
3. The password will not be forgotten by the party seeking authentication

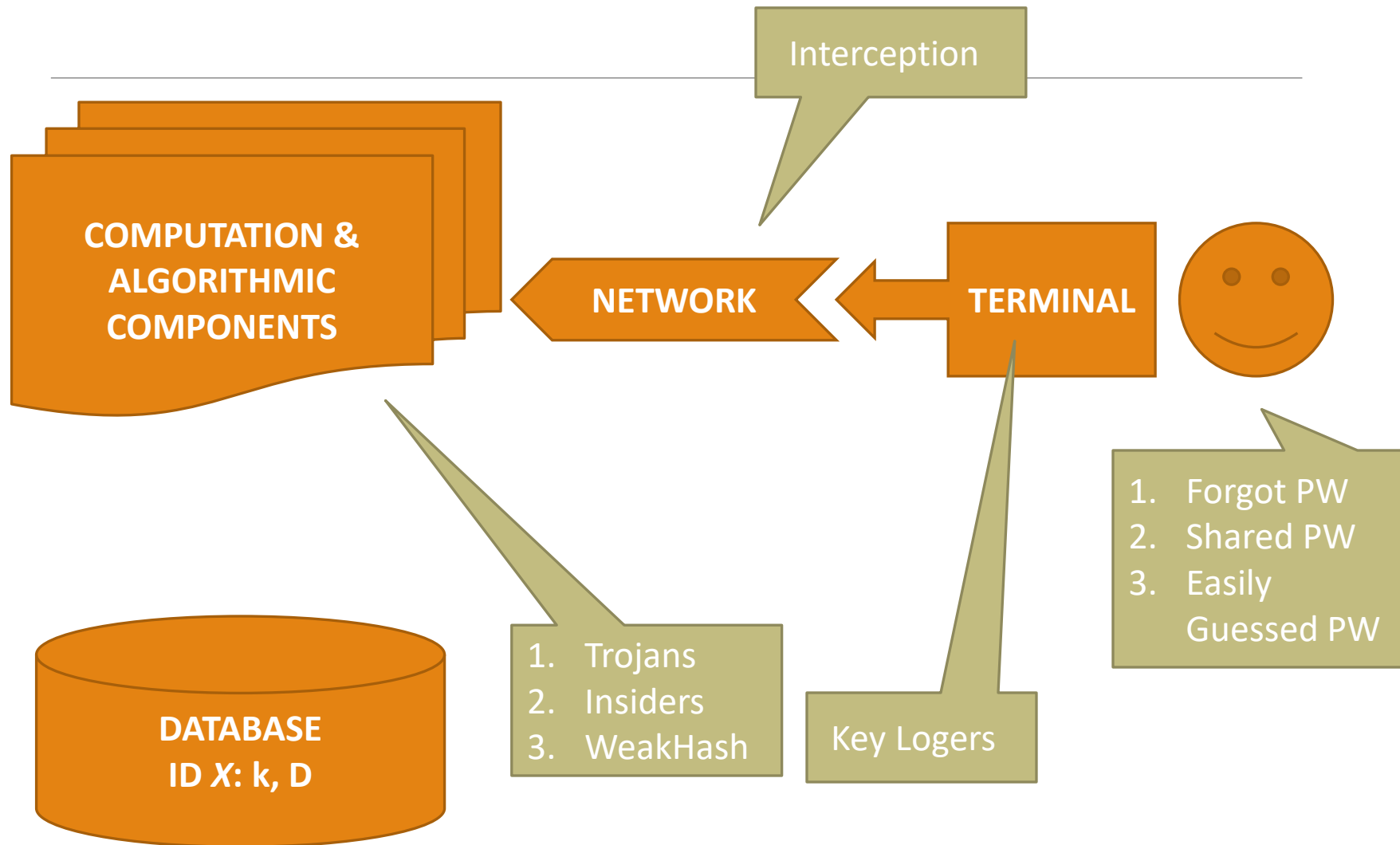
Password Registration



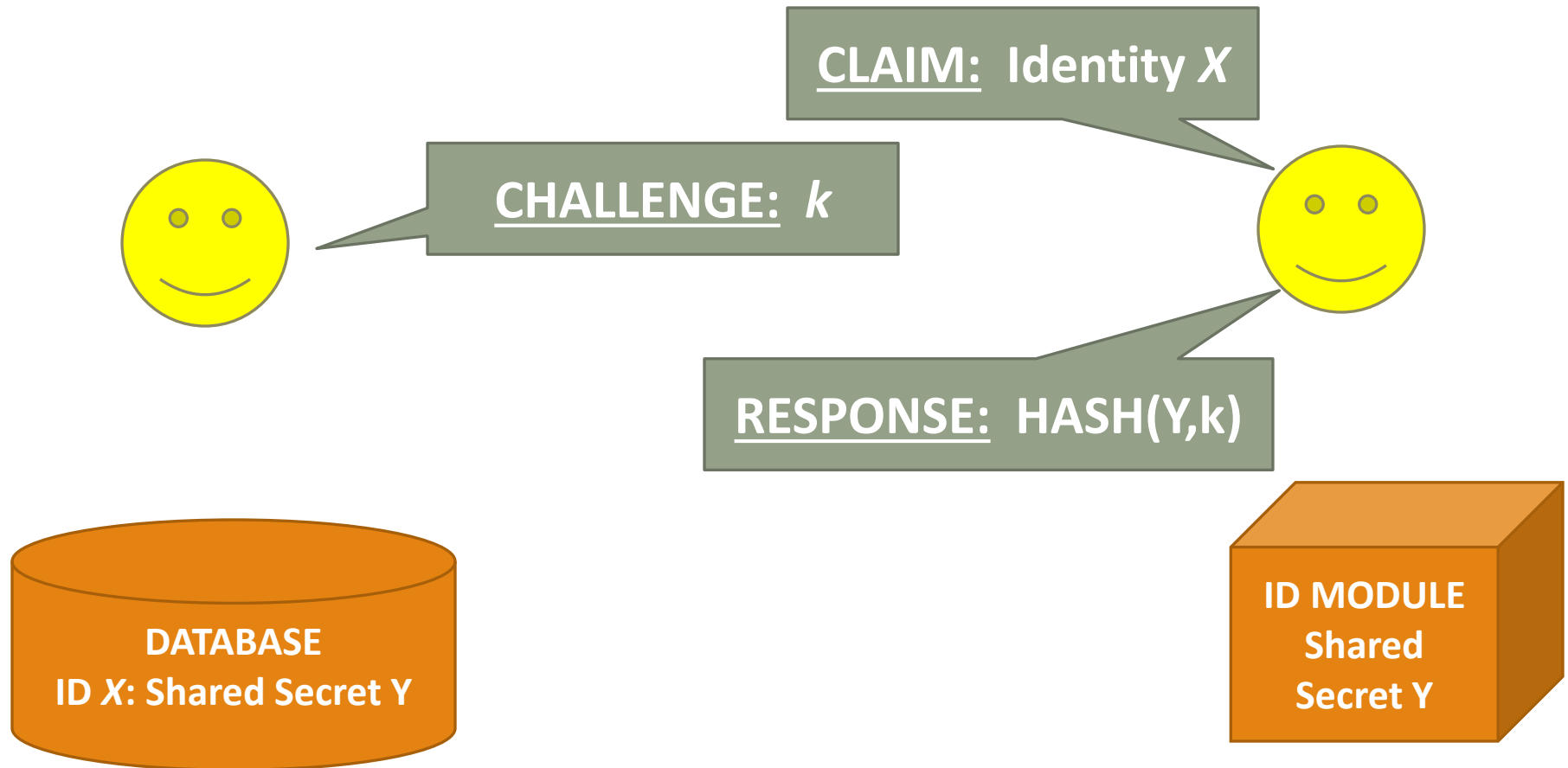
Password Verification



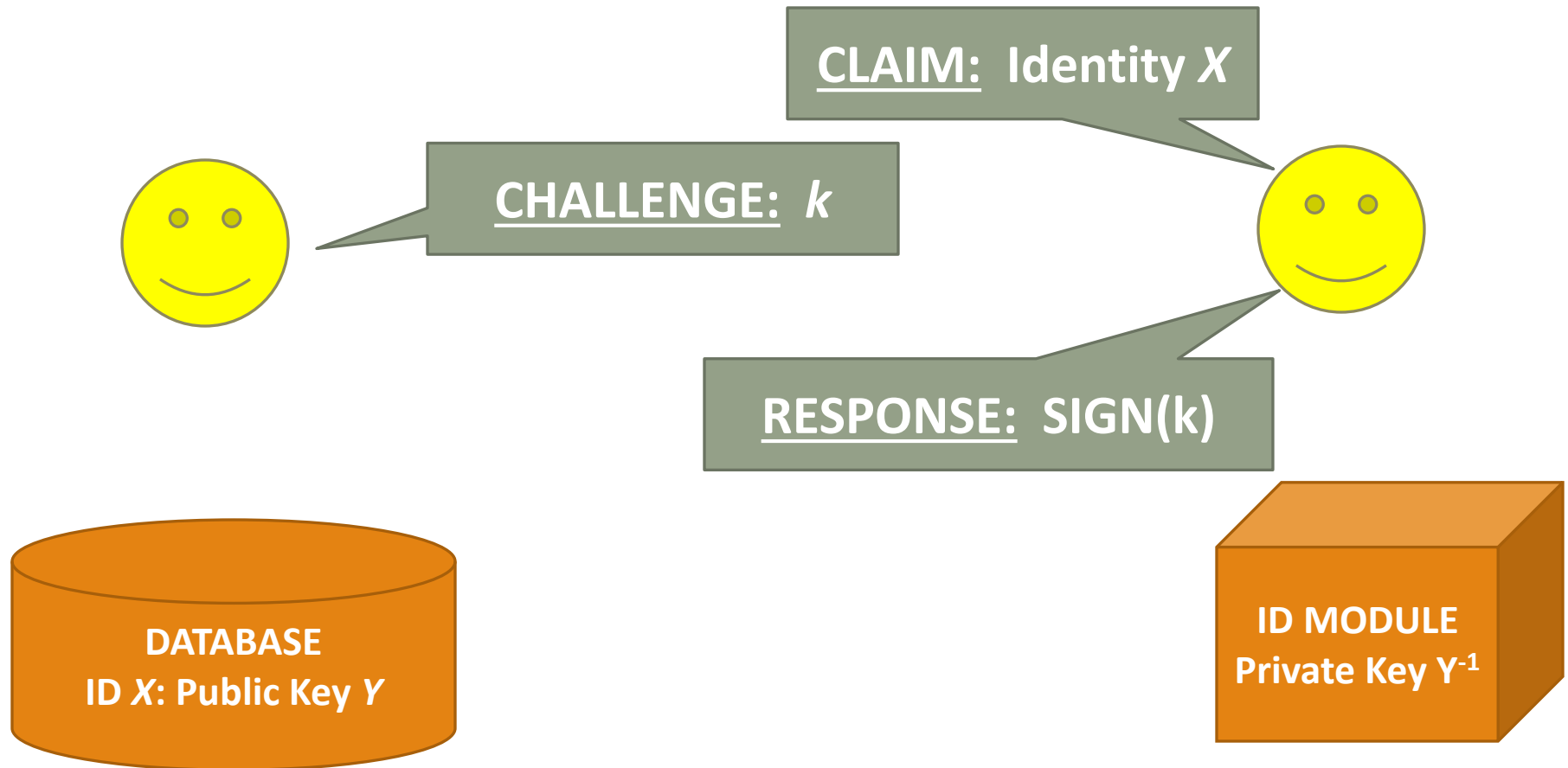
Common Problems



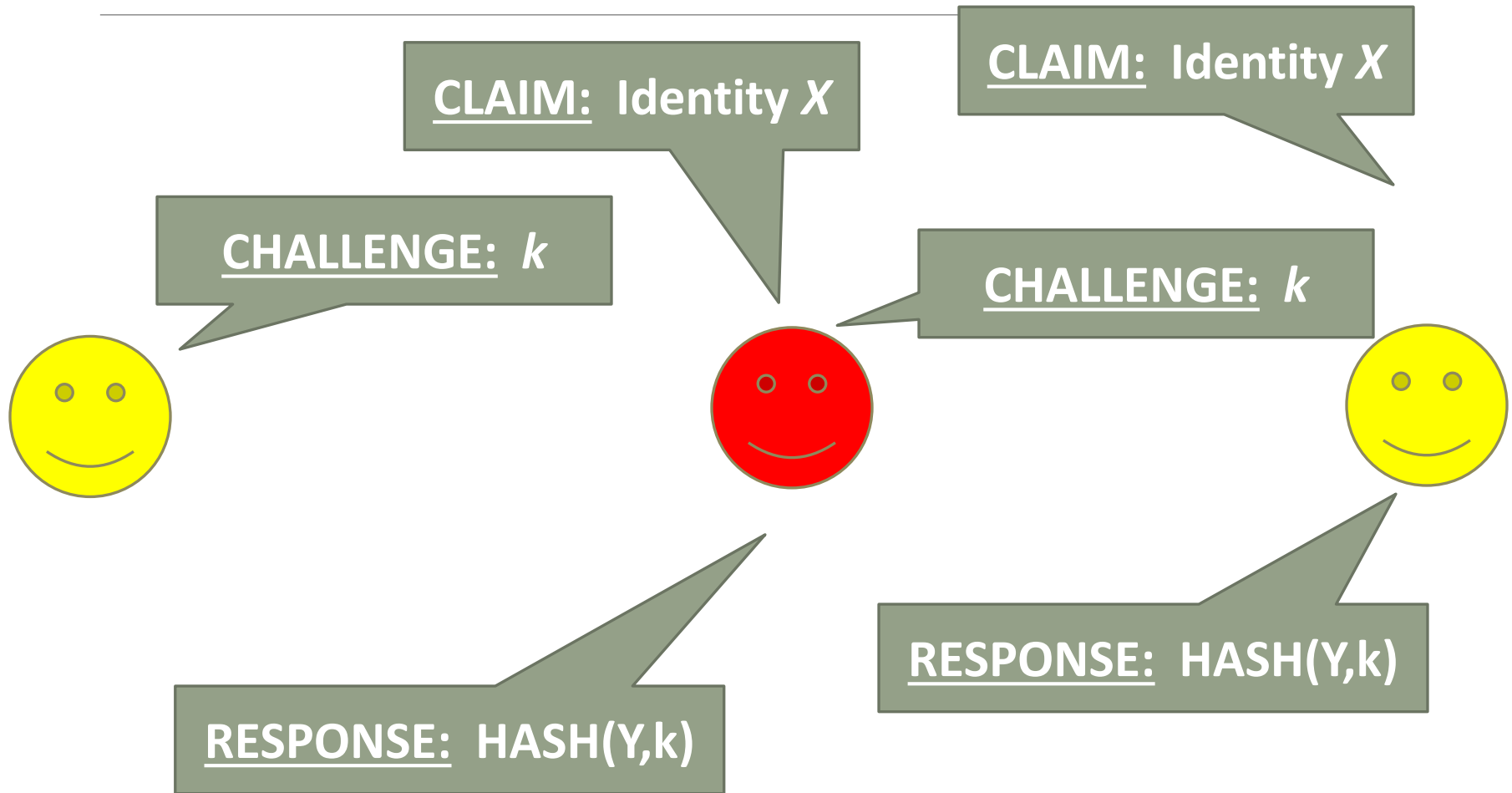
Challenge Response Symmetric



Challenge Response Asymmetric



Man-In-The-Middle (MITM)



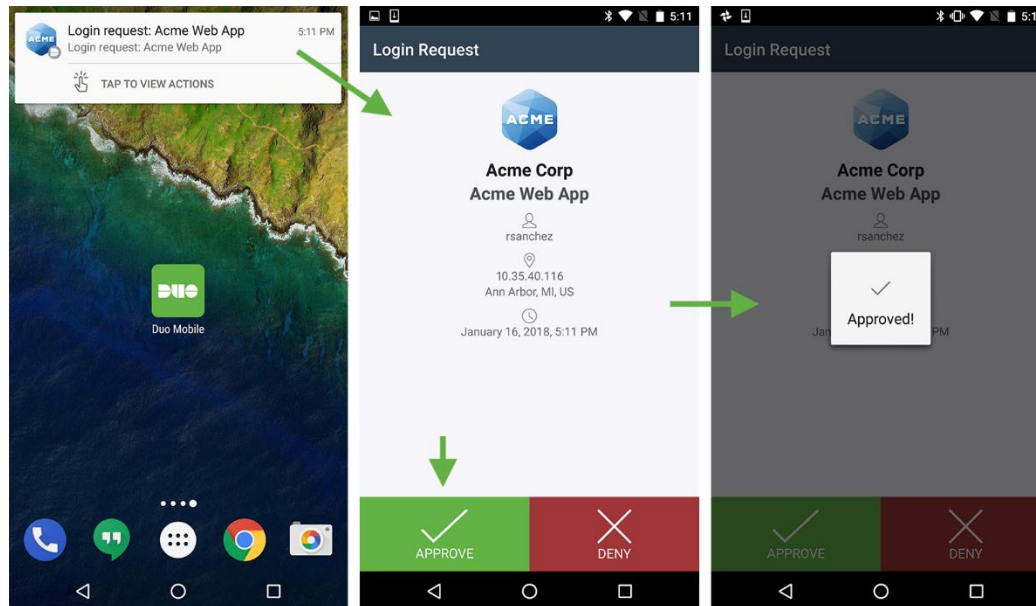
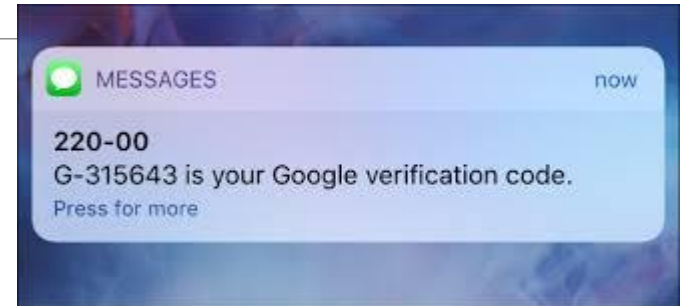


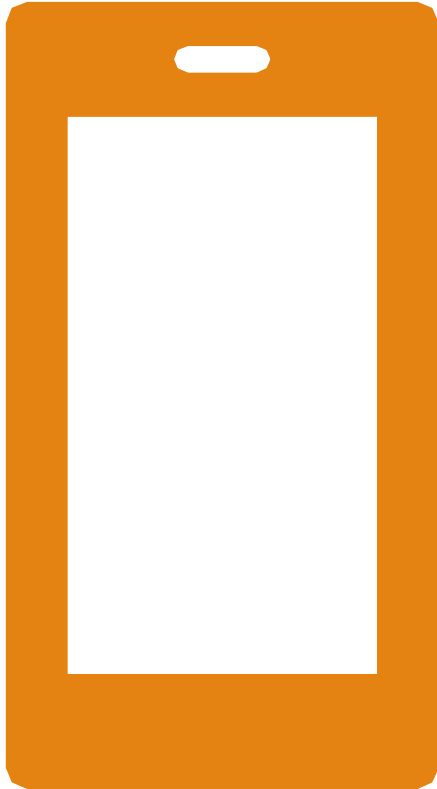
Something you Have

Security Assumptions

1. The “token” is ONLY possessed by the party seeking authentication
2. The token cannot be easily forged or duplicated
3. ***The authentication protocol is secure***

Something you Have Examples





Problems with “Tokens”

Is it **REALLY** something you have?

Is sending a code by email 2-factor?

What about phone cloning?

What about network interception?

Is an RSA Token's seed just
something you know?

“Something you can respond with”

Security Assumptions

- 1.The “characteristic” is effectively unique
- 2.Can effectively measure, record, or detect the characteristic
- 3.Characteristic cannot be forged, replicated, or otherwise “lost”
- 4.Characteristic will not change (too much) over time
- 5.Characteristic will never need to be revoked
- 6.The Authentication Protocol is Secure!**

Something
you Are

False Positives vs False Negatives



False Negative – Do not authorize party with valid characteristic



False Positive – Authorize party with invalid characteristic



Receiver Operating Characteristic

The trade off between FP and FN

Decreasing one typically increases the other

Equal Error Rate is when FP approximately equals FN

In most biometrics, ***False Negatives*** are worse

Problems with Biometrics

1. ~~Fingerprinting has been *seriously* misused in Courts (see Anderson at pp. 469-470)~~
2. ***Interpretation of results and understanding of statistics***
3. Variable accuracy in scanning mechanism
4. “Freshness”
5. Belief in infallibility leads to security culture problems
6. Biometrics exclude a *lot* of people (e.g., differently abled)
7. Civil Rights and Privacy issues
8. Injury that alter the characteristic (e.g., fingerprint)

One other “Authentication”

“Some**WHERE** you Are”

Almost universally used as an ancillary form of authentication

Generally used to **disprove rather than prove identity**

Complaints about KIZZA

1. Overstates strength of “something you are” authentication
2. “Client Authentication” (p. 214) – Not sure what he’s talking about
3. “Good” passwords are NOT vulnerable to brute force (p. 214)
4. Most passwords/secrets are not sent in the clear (p.215)
5. Challenge Response “problems” overstated/oversimplified (p. 216)
6. No deep discussion of Something you Have or Something you Are