# SOCIAL AUTHENTICATION FOR END TO END ENCRYPTION

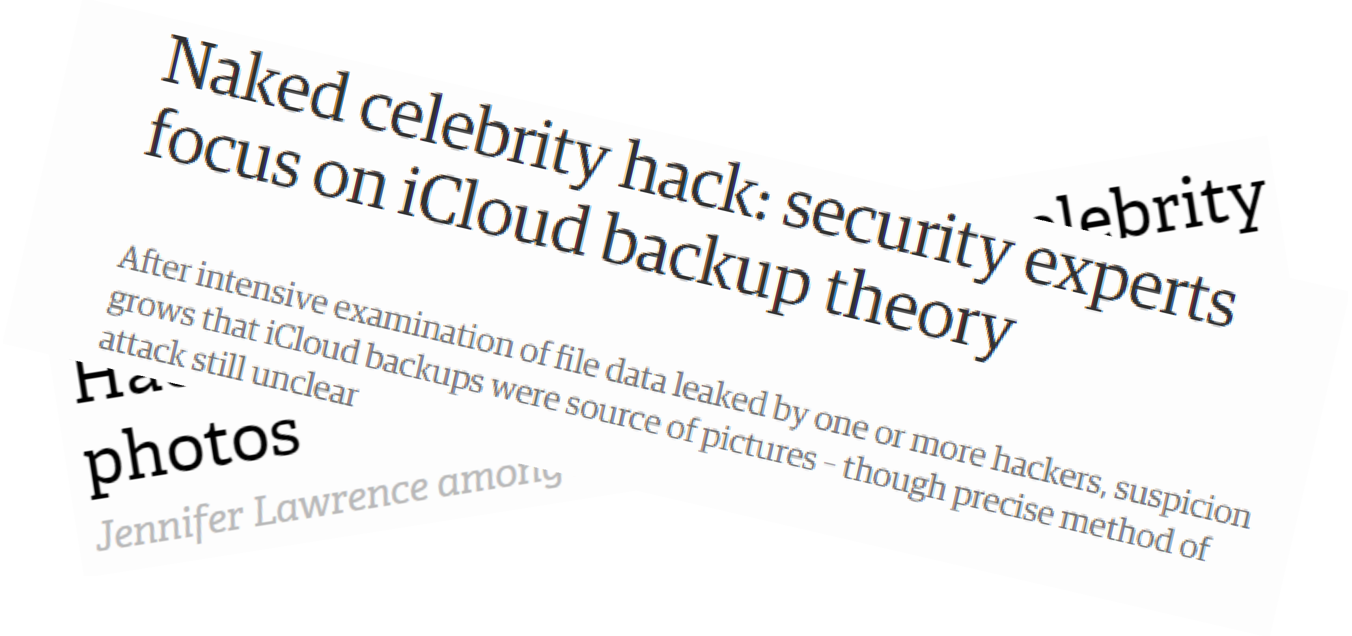
Elham Vaziripour, Mark O'Neill, Justin Wu, Scott Heidbrink, Kent Seamons, Daniel Zappala

Brigham Young University

# (IN)SECURITY AFFECTS LIVES

NEWS

**Hackers spied on 300,000 Iranians using fake Google certificate**



Naked celebrity hack: security experts focus on iCloud backup theory

After intensive examination of file data leaked by one or more hackers, suspicion grows that iCloud backups were source of pictures – though precise method of attack still unclear

lebrity

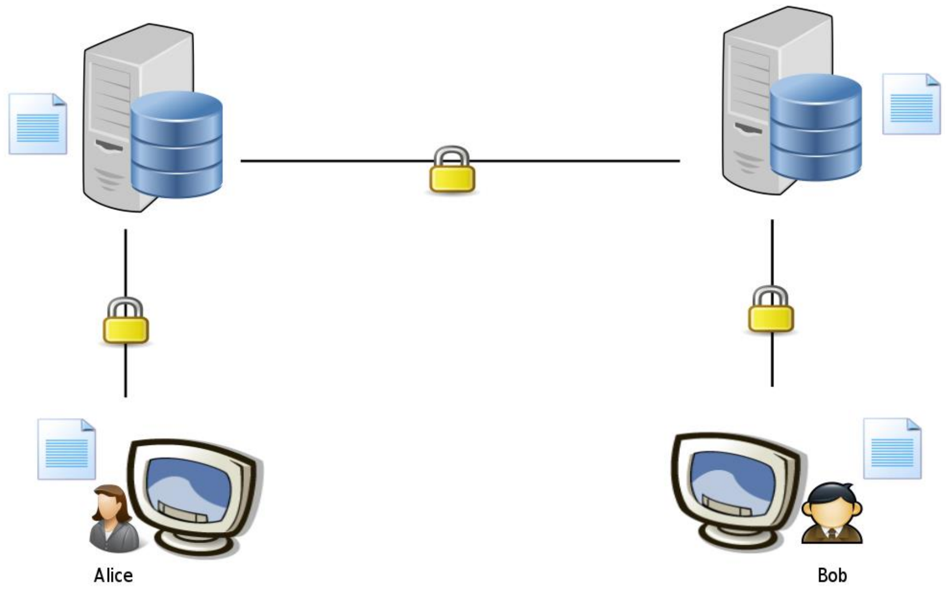
Ha

photos

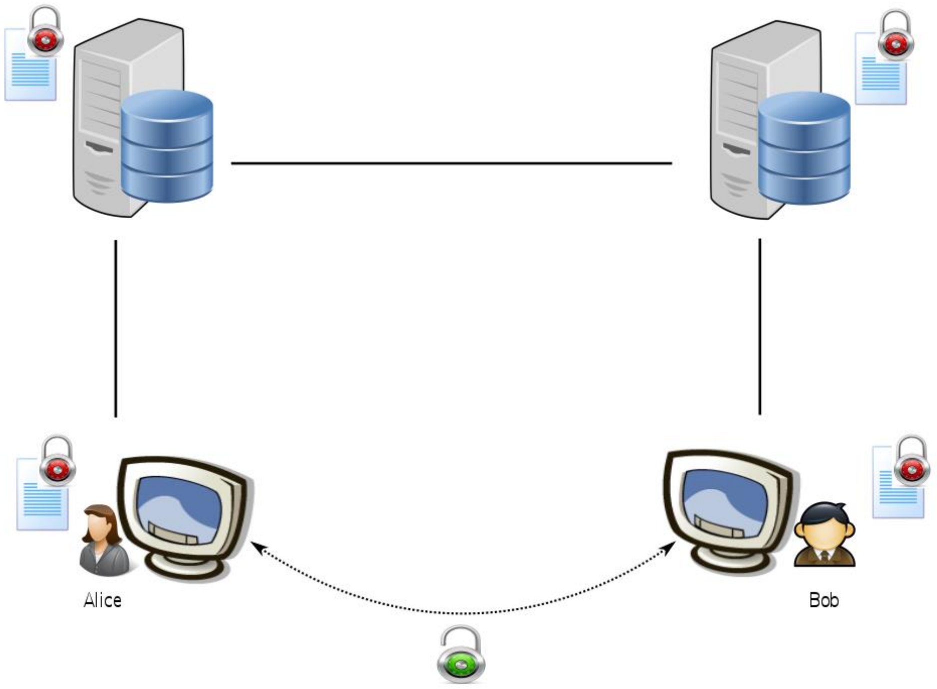
Jennifer Lawrence amon

# CONTENT-BASED ENCRYPTION

Connection-Based



Content-Based



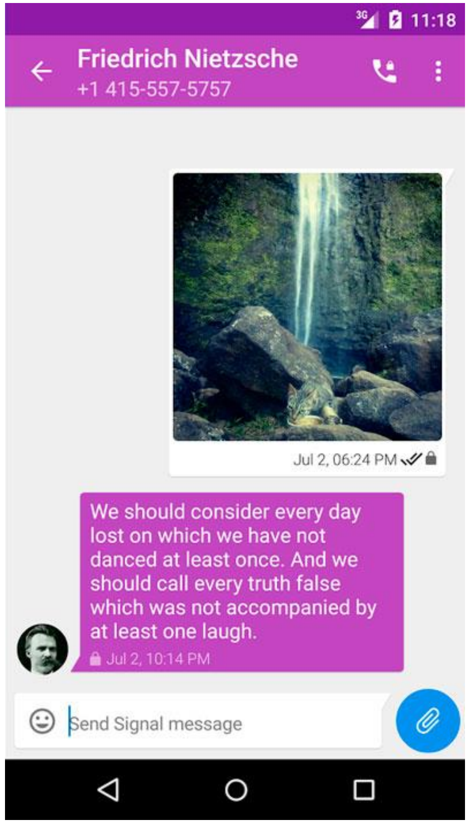
# SOME PROGRESS

Signal

ChatSecure

SafeSlinger

Keybase

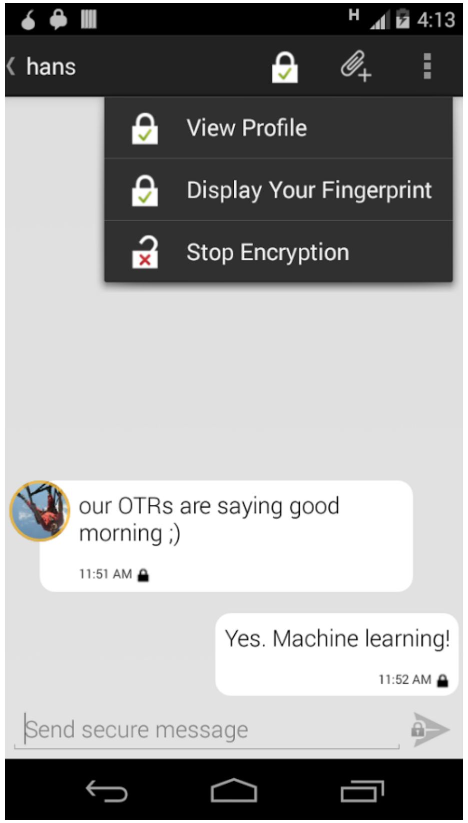


Jul 2, 06:24 PM

We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.

Jul 2, 10:14 PM

Send Signal message



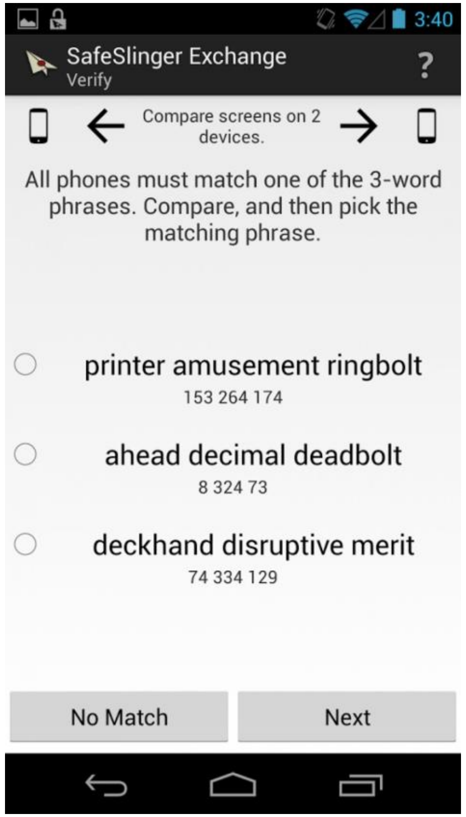
our OTRs are saying good morning ;)

11:51 AM

Yes. Machine learning!

11:52 AM

Send secure message



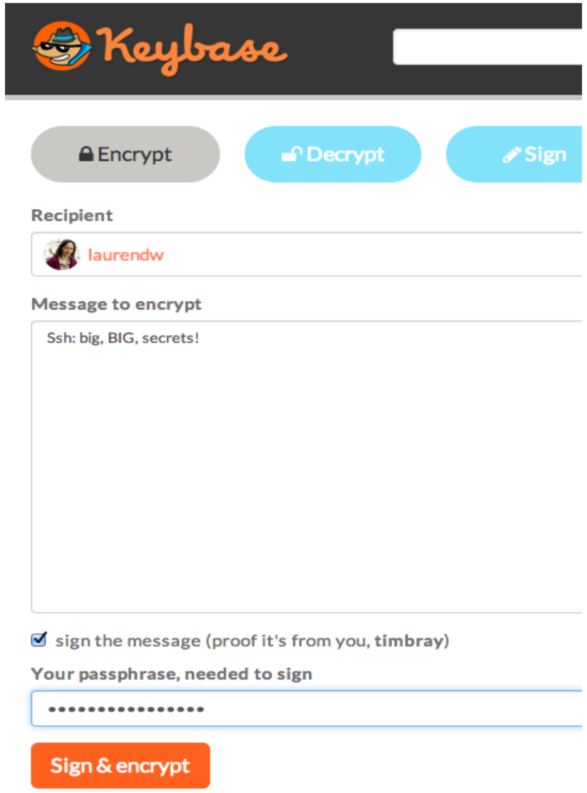
Compare screens on 2 devices.

All phones must match one of the 3-word phrases. Compare, and then pick the matching phrase.

○ printer amusement ringbolt
153 264 174

○ ahead decimal deadbolt
8 324 73

○ deckhand disruptive merit
74 334 129



Recipient

laurendw

Message to encrypt

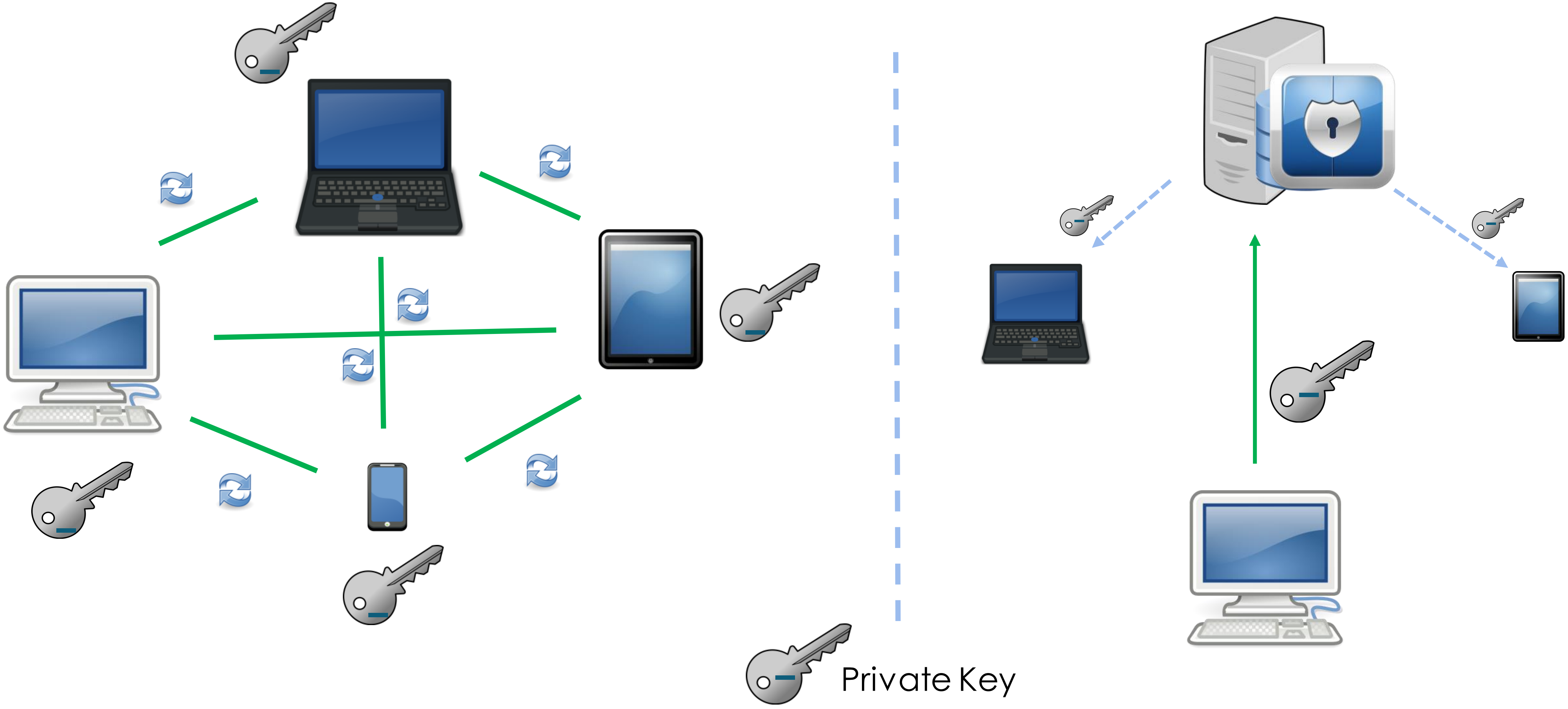
Ssh: big, BIG, secrets!

☑ sign the message (proof it's from you, timbray)

Your passphrase, needed to sign

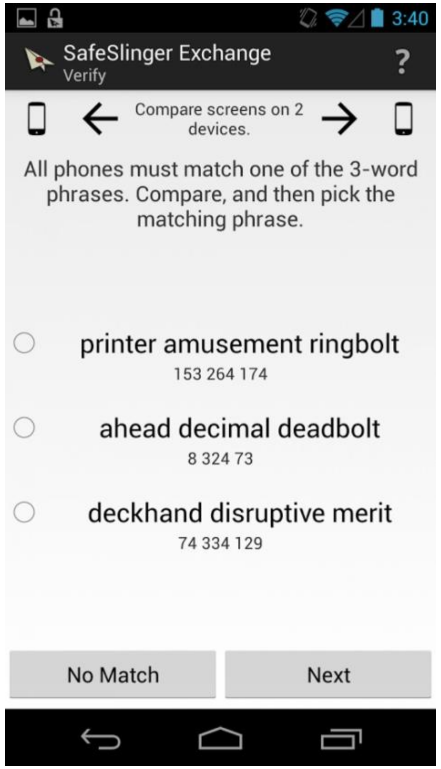
••••••••••••••••

# PROBLEM #1: KEY PORTABILITY



# PROBLEM #2:
# KEY DISTRIBUTION AND TRUST

Key Signing Parties



3:40

SafeSlinger Exchange
Verify

Compare screens on 2 devices.

All phones must match one of the 3-word phrases. Compare, and then pick the matching phrase.

○ printer amusement ringbolt
153 264 174

○ ahead decimal deadbolt
8 324 73

○ deckhand disruptive merit
74 334 129

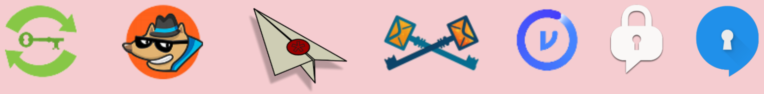
No Match | Next

Manual Inspection

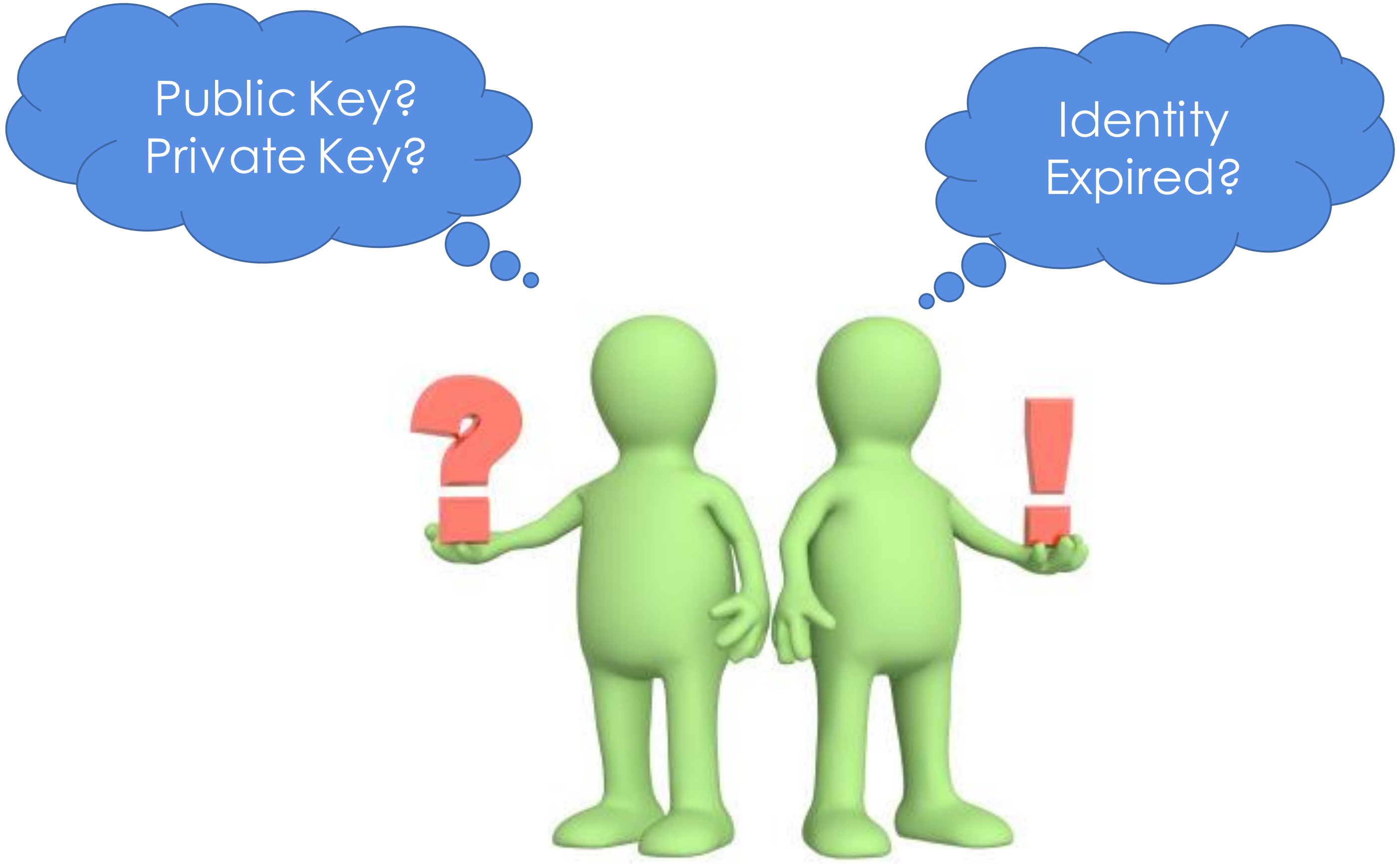
GlobalSign
Entrust®
VeriSign®
digicert®
StartCOM SSL SECURED
COMODO
Creating Trust Online™
CNNIC
中国互联网络信息中心
U.S. DEPARTMENT OF HOMELAND SECURITY
+ 1500 More
GoDaddy™
DigiNotar
Internet Trust Services

Certificate Authorities

# PROBLEM #3: GENERALITY

| Type | Support |
|---|---|
| SMS | |
| Voice | |
| IM | |
| Email | |
| Web | |
| Video | |
| Key Mgmt. |  |

# PROBLEM #4: USABILITY



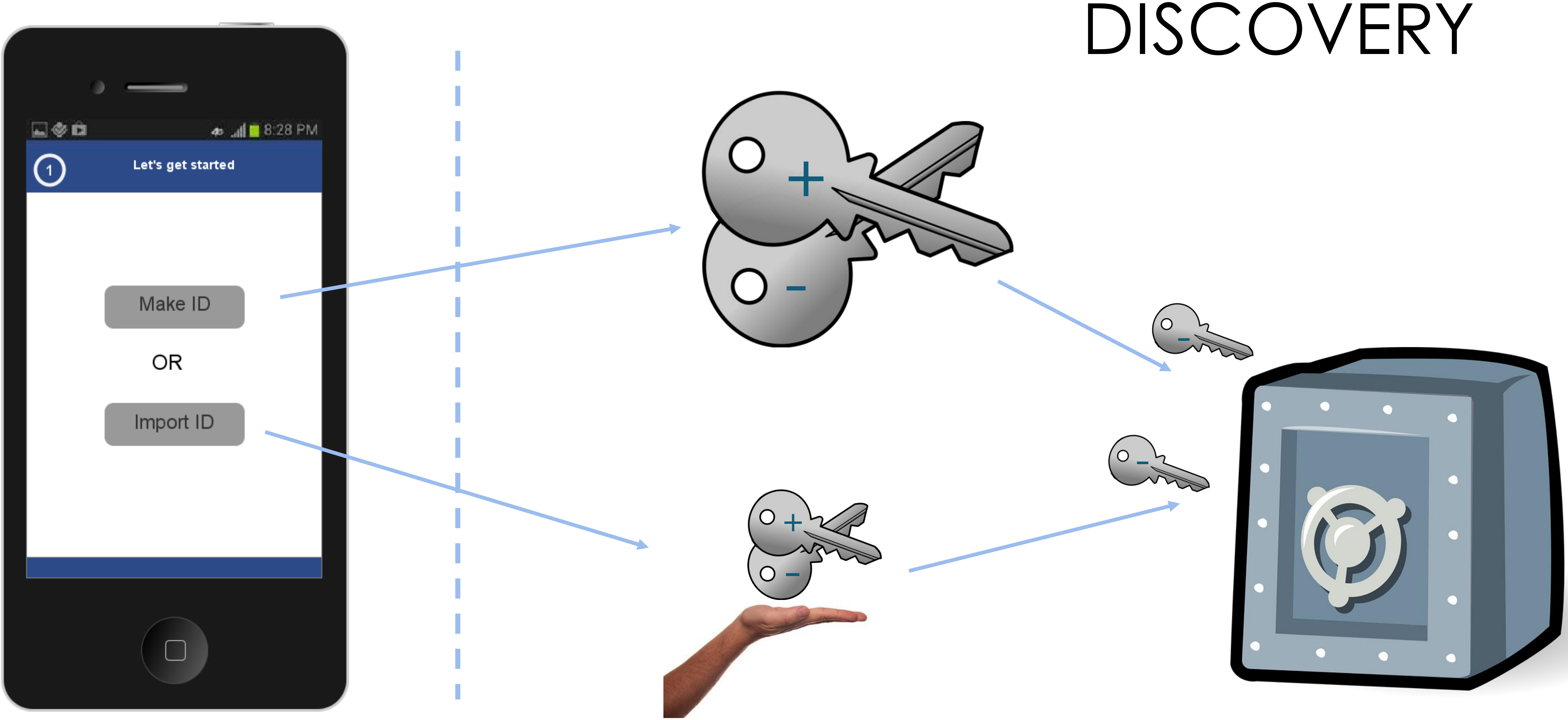
Public Key?
Private Key?

Identity
Expired?

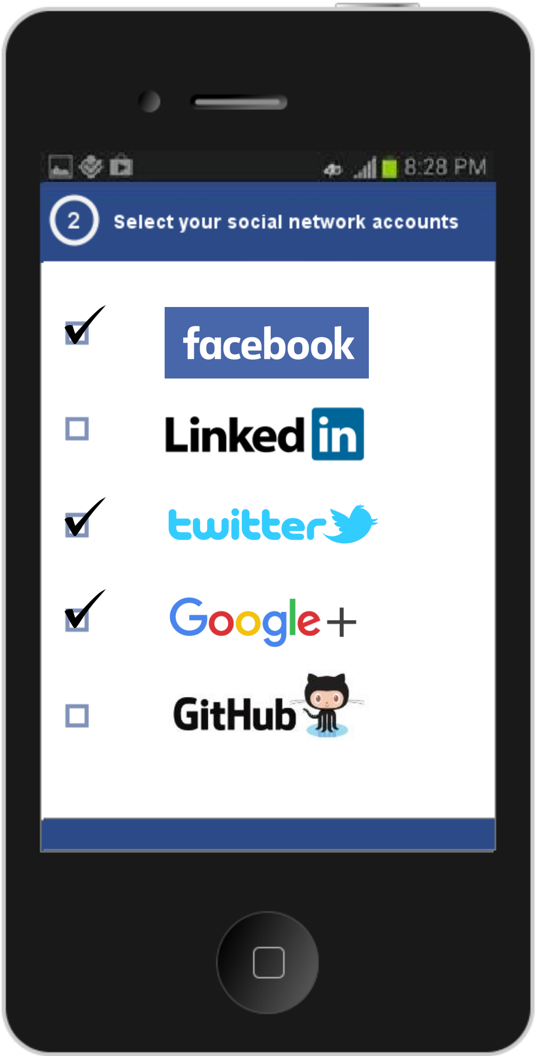
# USERS NEED…

1. A portable, secure private key store
2. A way to automatically manage public keys
    - Discovery
    - Update
    - Validation
3. A general service for encryption/decryption and signing/verifying
    - For arbitrary types of communication
    - Interoperable with other apps
4. **Usability** for all this!

# KEY PUBLICATION AND DISCOVERY



# KEY PUBLICATION AND DISCOVERY



2 Select your social network accounts

☑ facebook

□ LinkedIn

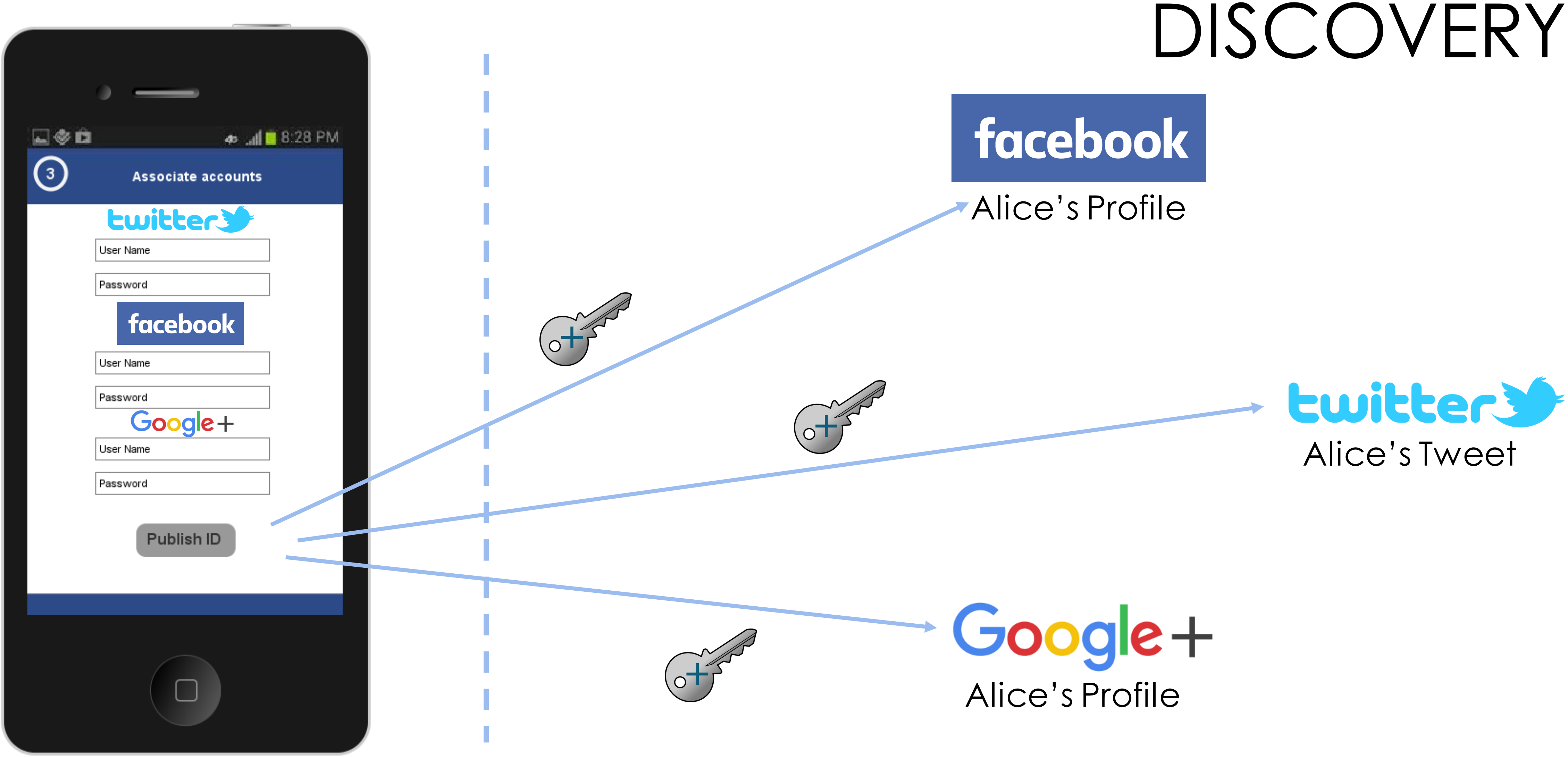
☑ twitter

☑ Google+

□ GitHub

- ✓ facebook
- ✓ twitter
- ✓ Google+

# KEY PUBLICATION AND DISCOVERY

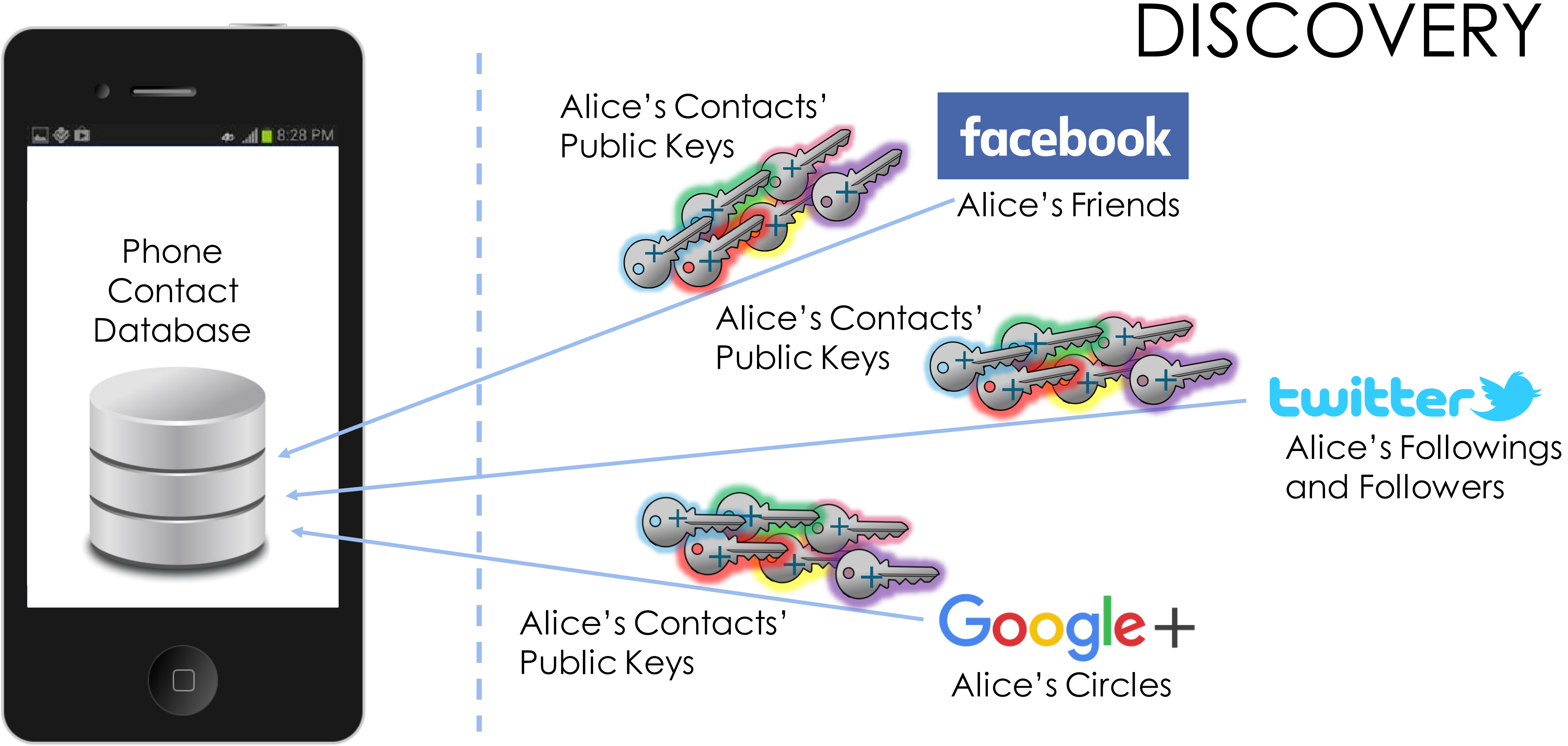


Alice’s Profile

Alice’s Tweet

Alice’s Profile

# KEY PUBLICATION AND DISCOVERY



Phone Contact Database

Alice’s Contacts’ Public Keys

Alice’s Friends

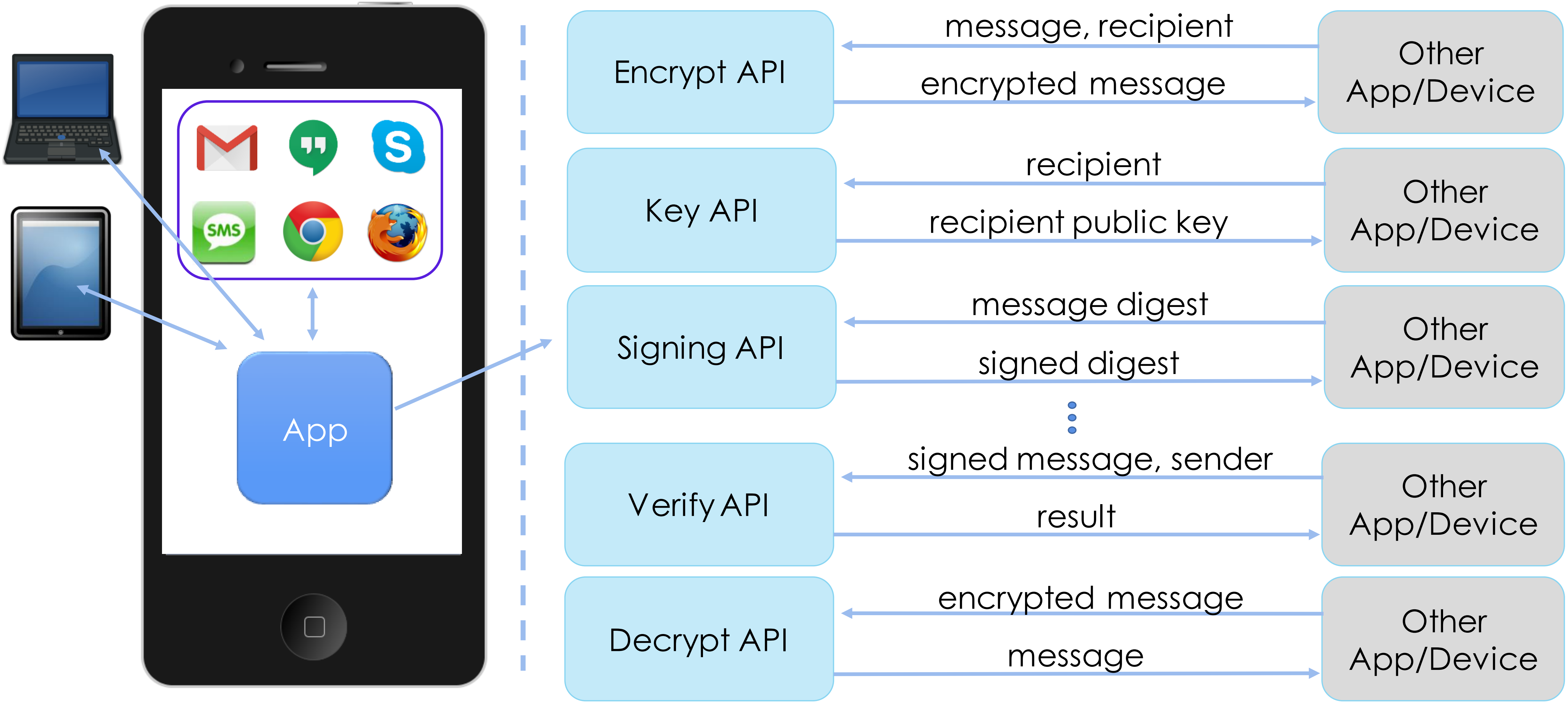
Alice’s Contacts’ Public Keys

Alice’s Followings and Followers

Alice’s Contacts’ Public Keys

Alice’s Circles

# SOCIAL AUTHENTICATION API



# POINTS OF DISCUSSION

- Usable Key Management
    - User key revocation
    - User key updating
    - Automatically receive updates about key changes via periodic checks of OSN data
- Inducting Novices
    - Leveraging OSN
- Authenticating a Stranger
    - Add them as a “friend” on one or more OSNs, immediately receive their public key
- Attack modeling
    - Evaluate resilience to attacks such as Sybil attack