Recent developments in secure messaging

(and other person-to-person communication)

Trevor Perrin

SOUPS 2014

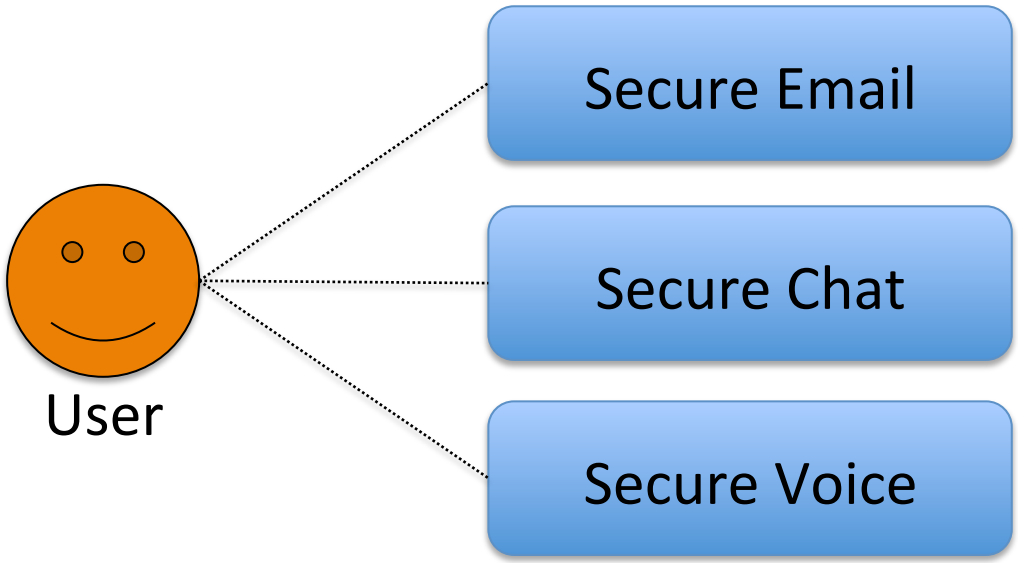
Security Model

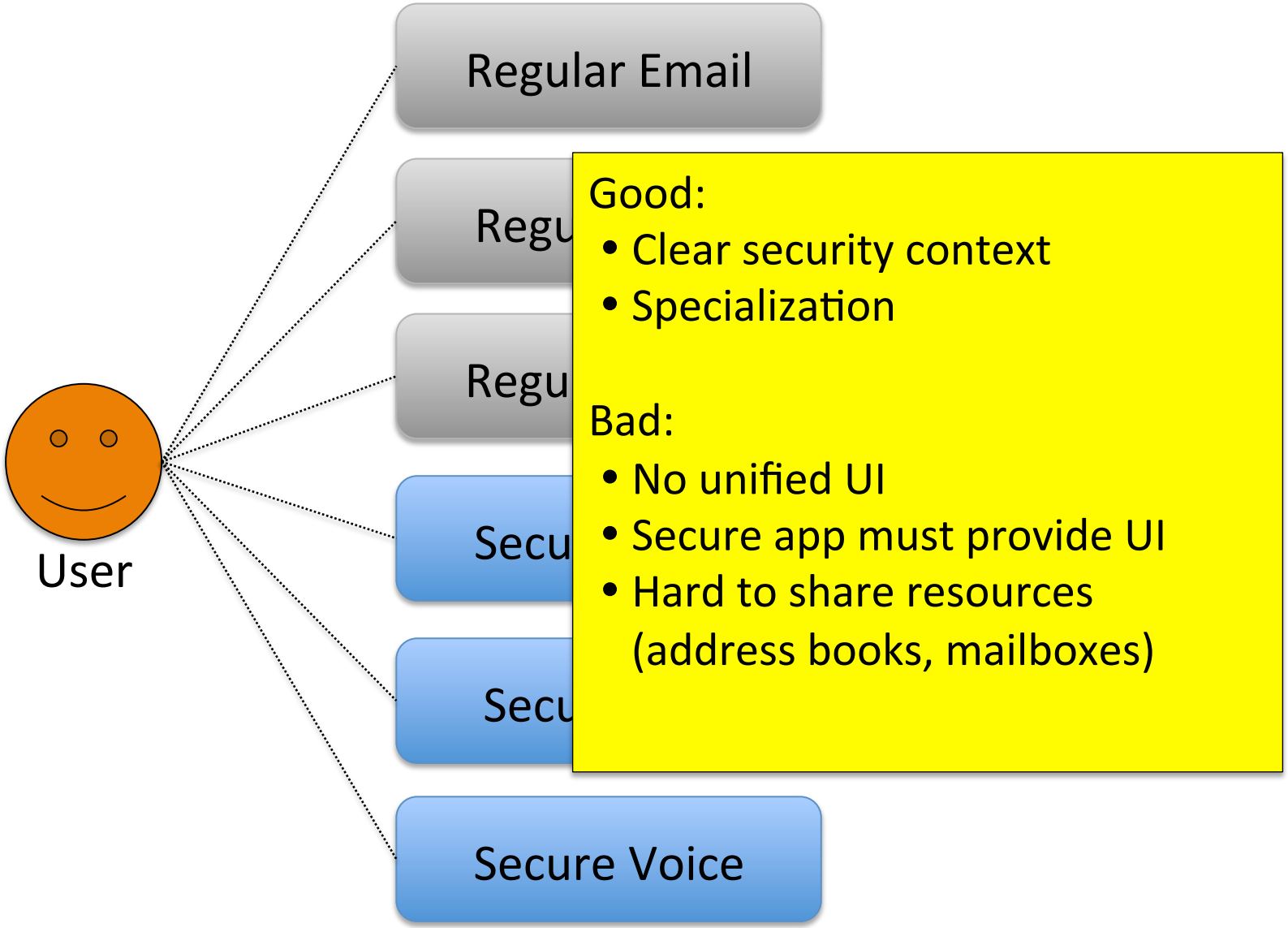
- No trust in 3rd parties

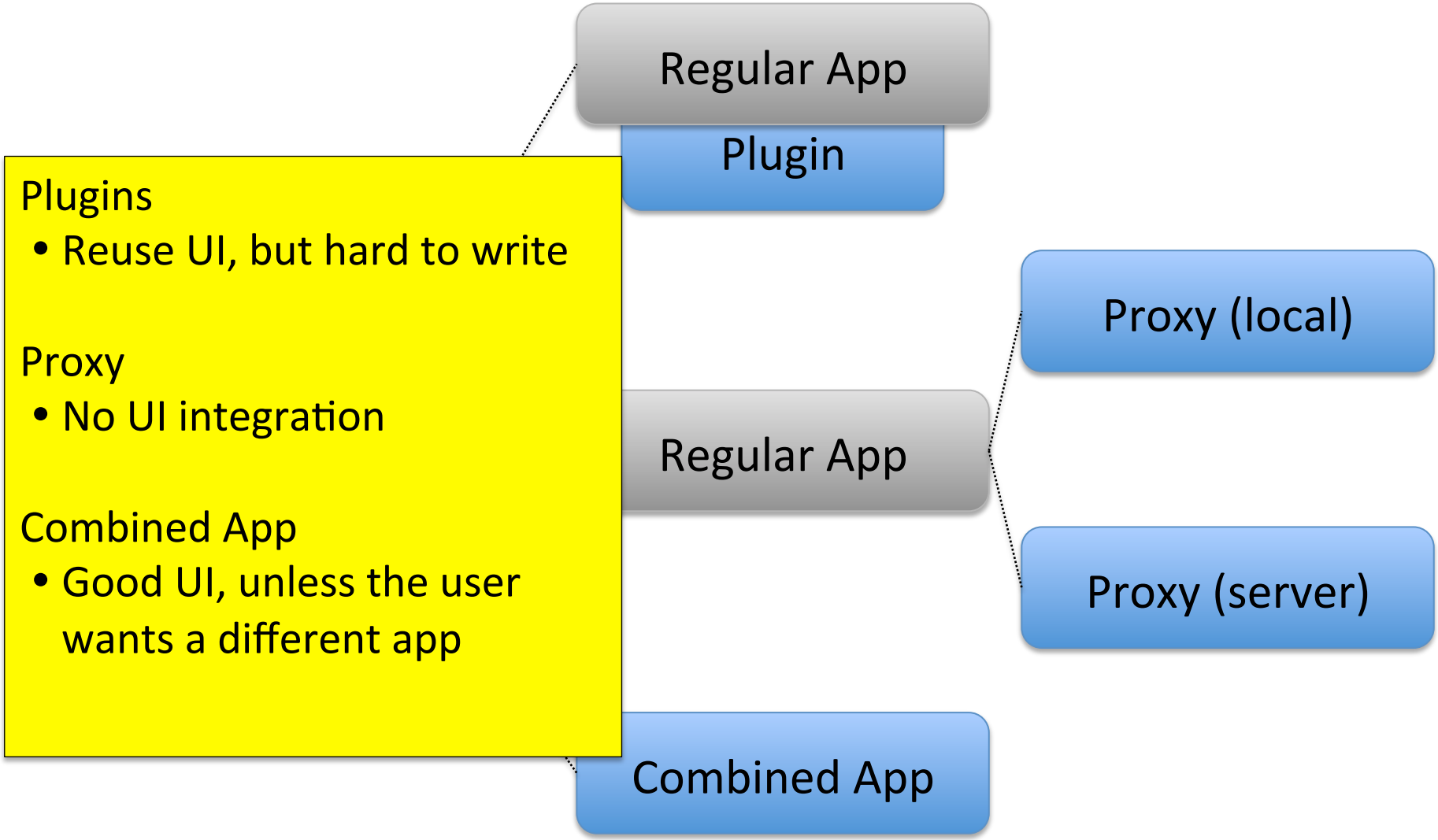
- Better: Trust in 3rd parties is
  - Optional
  - Agile
  - Minimal

Security Goals

- Confidentiality
  - Contents
  - Relationships and Identities
- Authentication
- Integrity
  - Contents
  - Multi-message and multi-party conversations

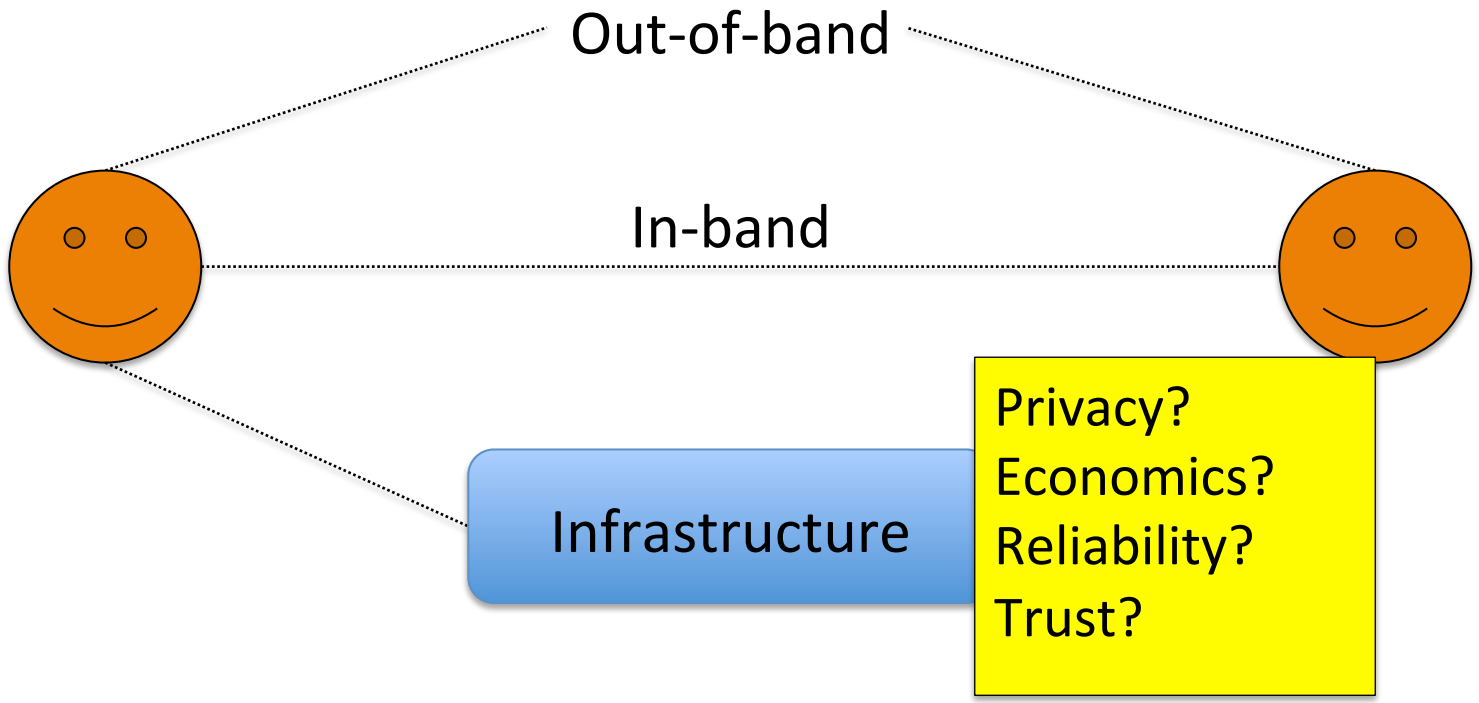

Secure Email
Secure Chat
Secure Voice
User


Regular Email
Regu
Regu
Secu
Secu
Secure Voice
User
Good:
• Clear security context
• Specialization
Bad:
• No unified UI
• Secure app must provide UI
• Hard to share resources
(address books, mailboxes)

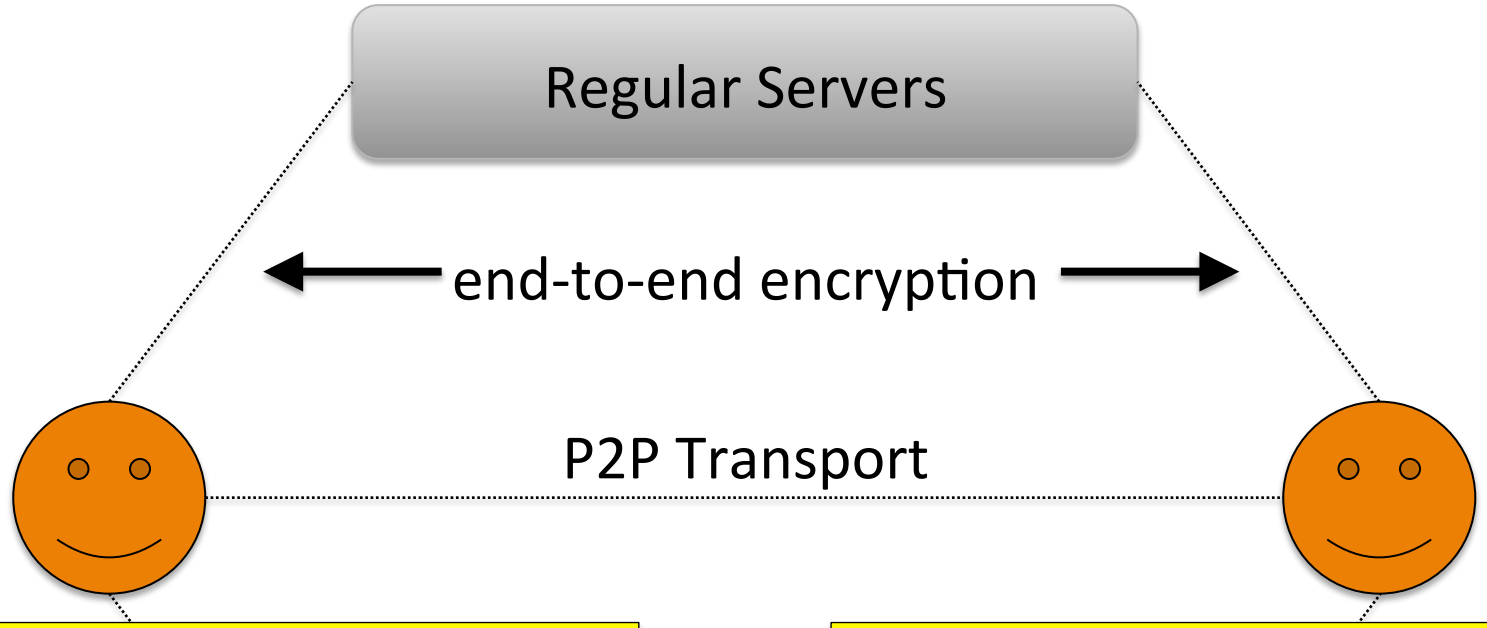

Regular App
Plugin
Plugins
• Reuse UI, but hard to write
Proxy
• No UI integration
Combined App
• Good UI, unless the user wants a different app
Proxy (local)
Regular App
Proxy (server)
Combined App

Signalling

- Contact discovery
- Key discovery and authentication
- Presence and routing



Transport



Tolerant of encryption?

Spam / malware filtering?

Identity / relationship hiding?

ure Ser

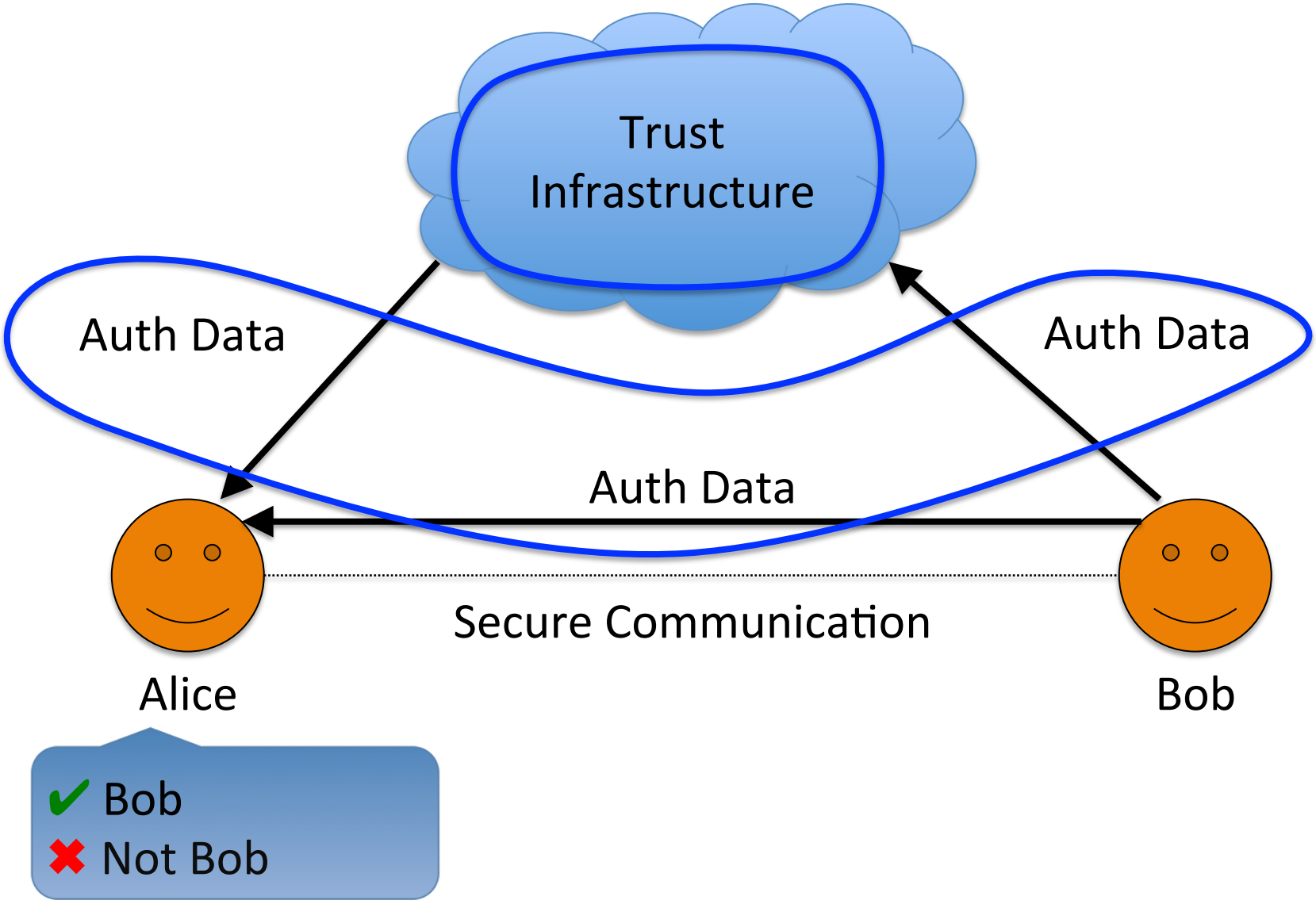
Reliability tradeoffs

Confidentiality

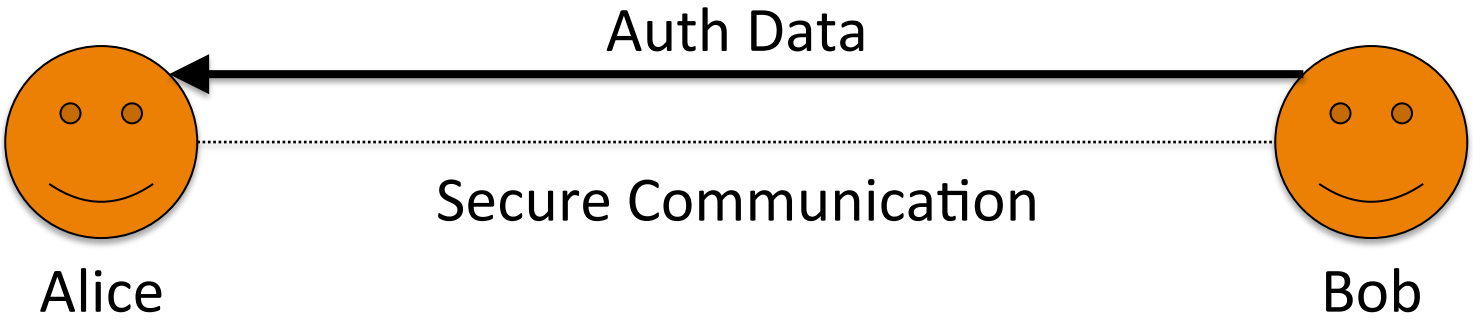
- Less info lea
- More leake

Economics?
Reliability?
Trust?

Authentication

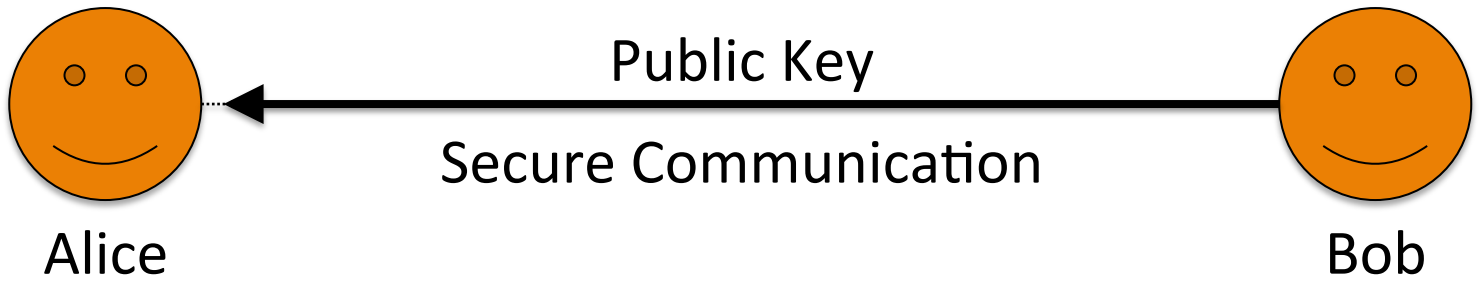


Authentication Data



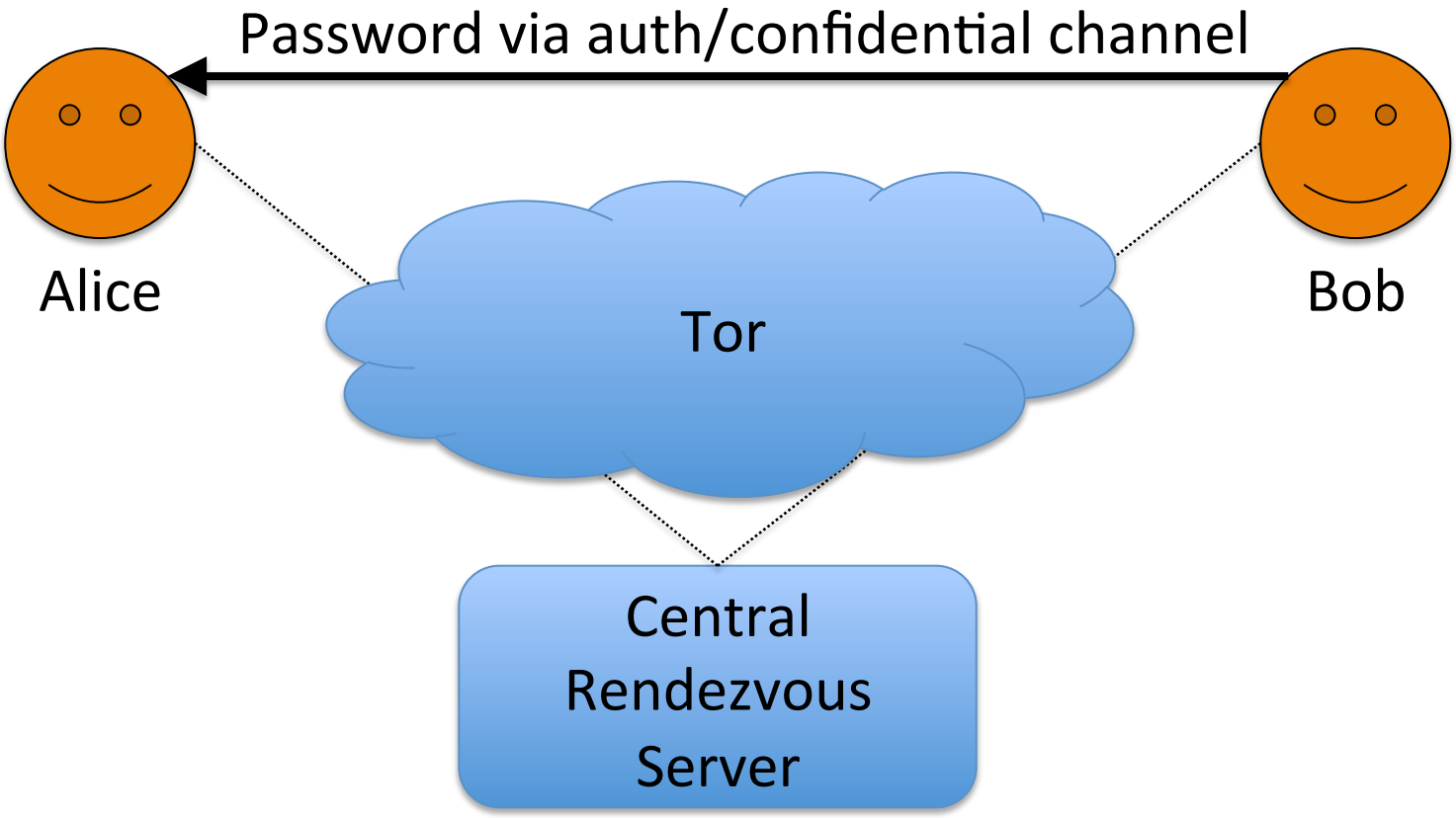
- Needs usability AND security

Observational Trust



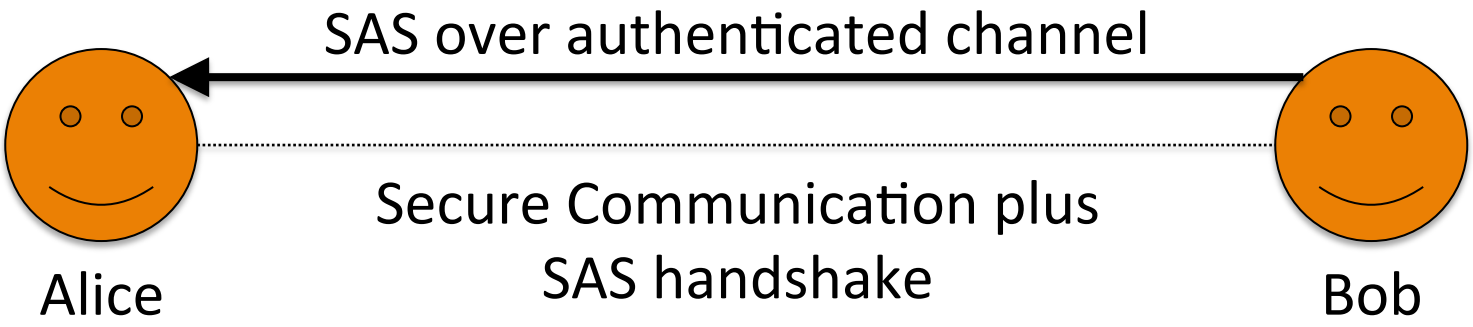
- Remember key, warn on change
- Key continuity, “TOFU”
- Gets better the more you do

Passwords



Messages exchanged via password-derived meeting ID

Short Auth Strings



Alice → Bob: $Hash(DH_A)$

Alice ← Bob: DH_B

Alice → Bob: DH_A

SAS = $Hash(DH_A \,||\, DH_B)$, e.g. “goldfish Medusa”

Public-Key Fingerprints

exult - wish - skin - envoy - jenny - basin - apron - gulp - roon

C4E40F71 A92175F8 597A29A 4FF

the wire repeats after hi

gives belov

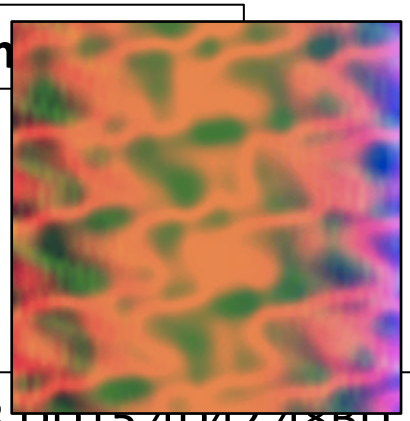
ne laughs

kindly

wfXhb

0371 8373 DD15 4D42 48BD

```
+--[ RSA 2048]----+
|         o=.     |
|      o  o++E    |
|     + . Ooo.    |
|      + O B..    |
|       = *S.     |
|        o        |
|                 |
|                 |
|                 |
+-----------------+
```



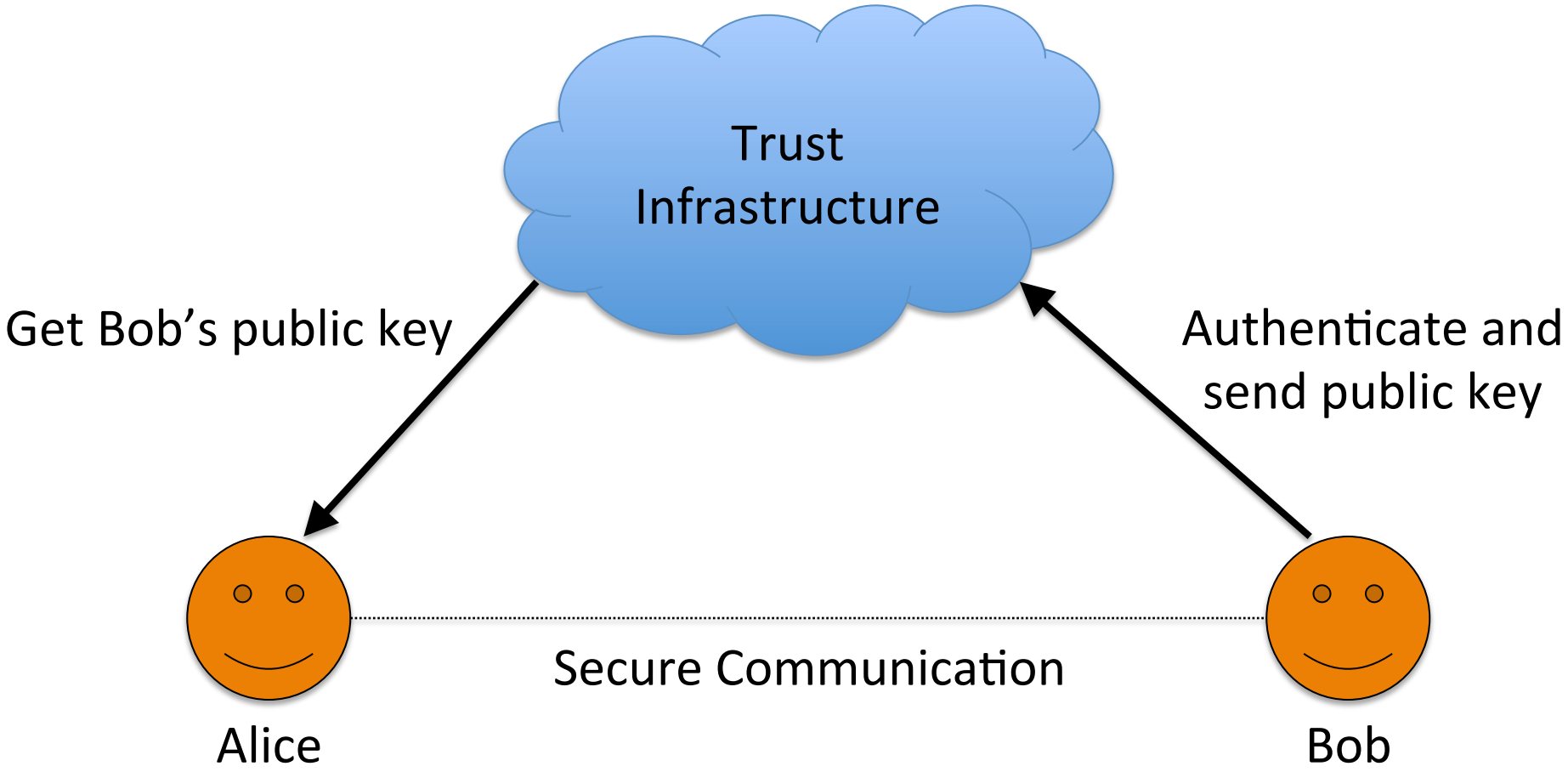
co hamrock -

ou Norwegian - tactics - unravel - reward -

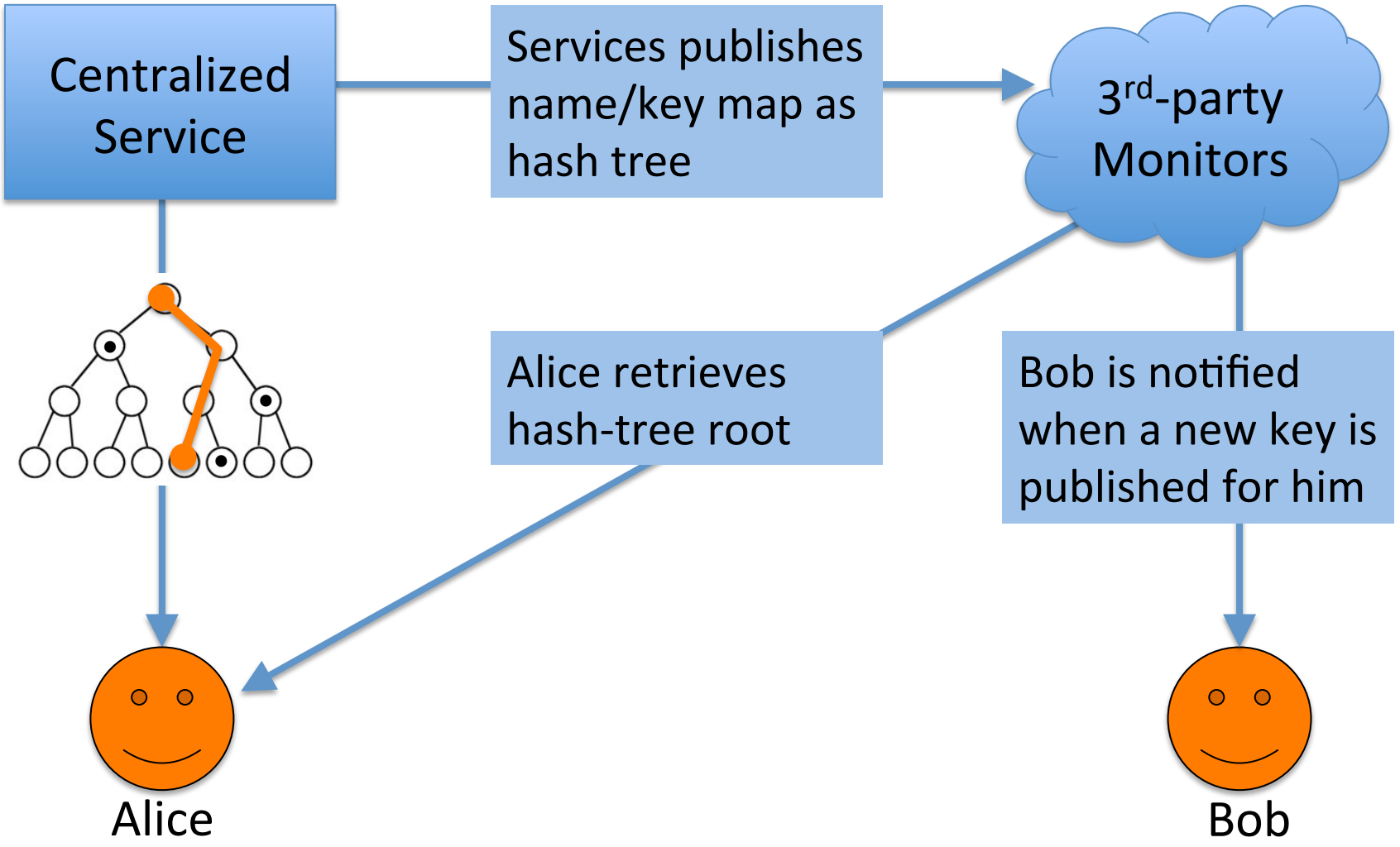
decadence - orca - antenna - sweatband - consensus

9:b1:0f:66:73:a8

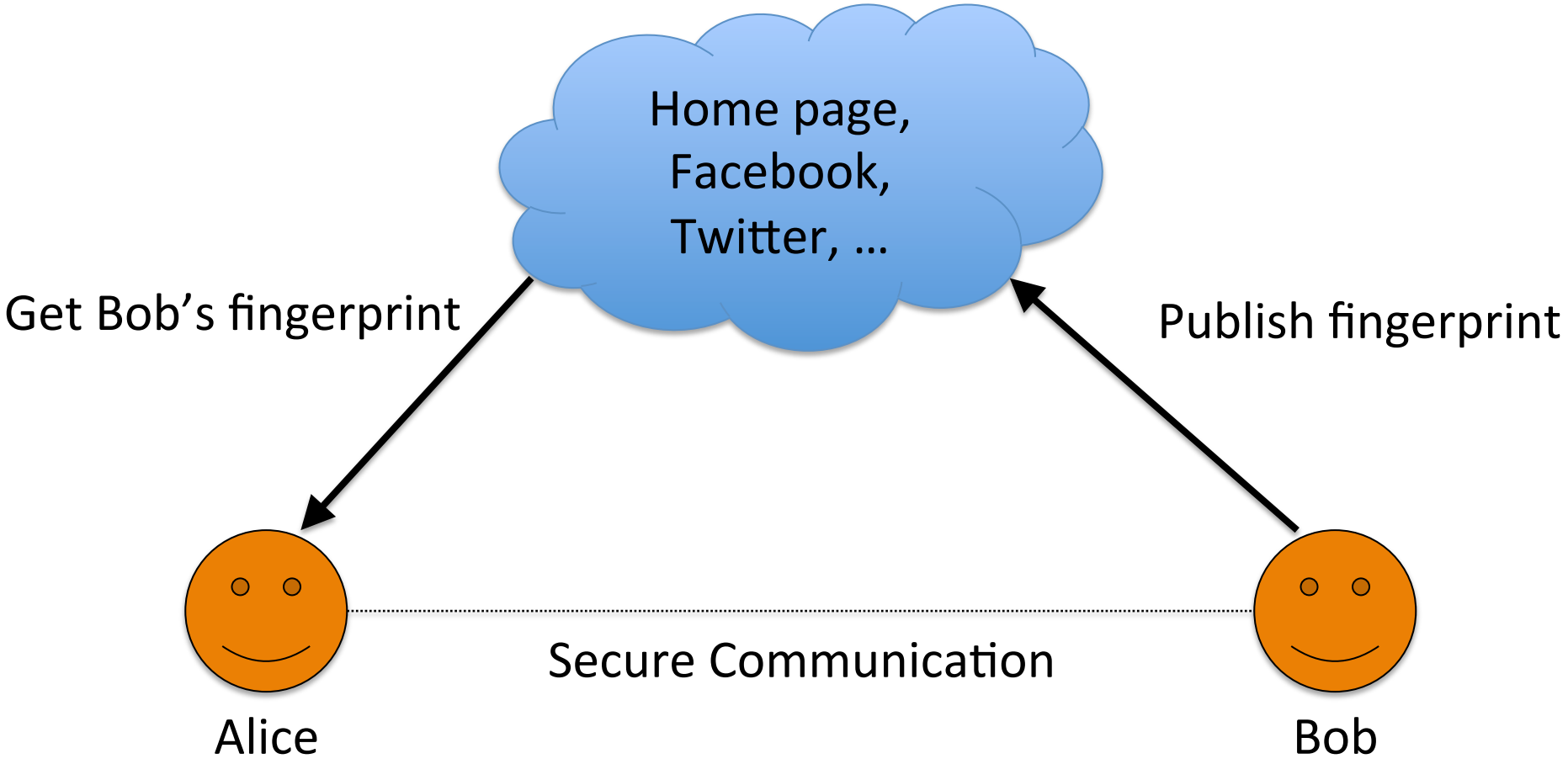
lae - zibo - salewi


Trust
Infrastructure
Get Bob's public key
Authenticate and
send public key
Secure Communication
Alice
Bob

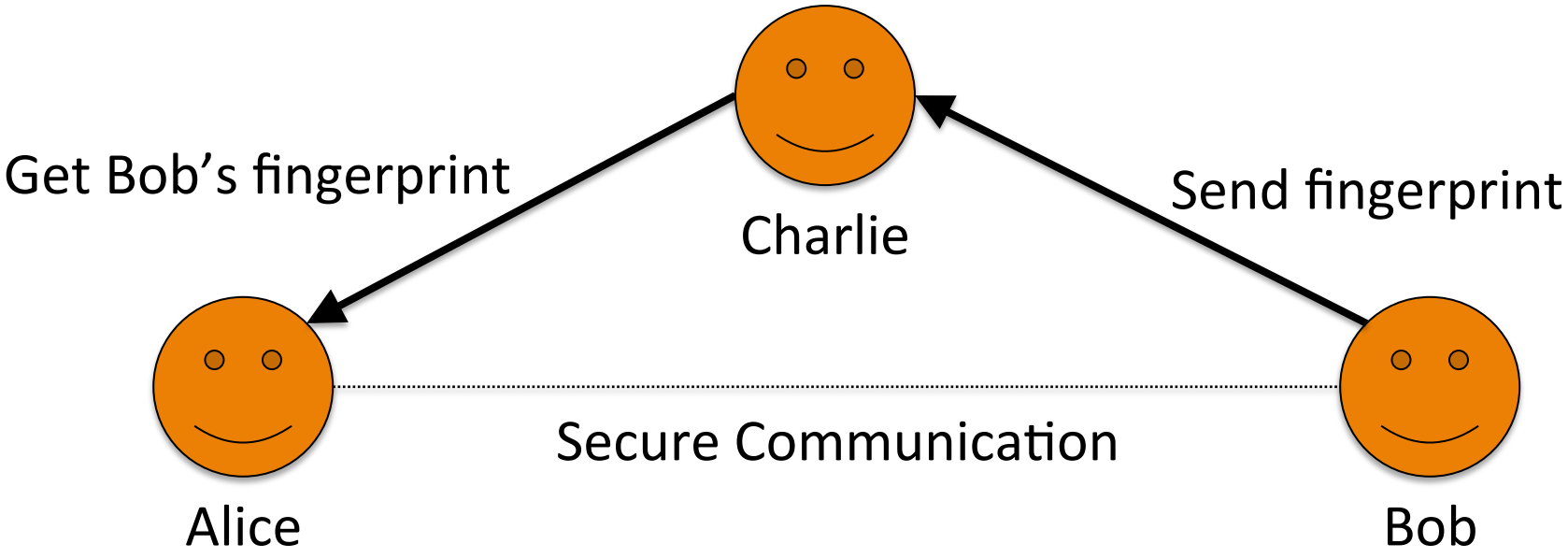
Certificate Transparency (adapted)



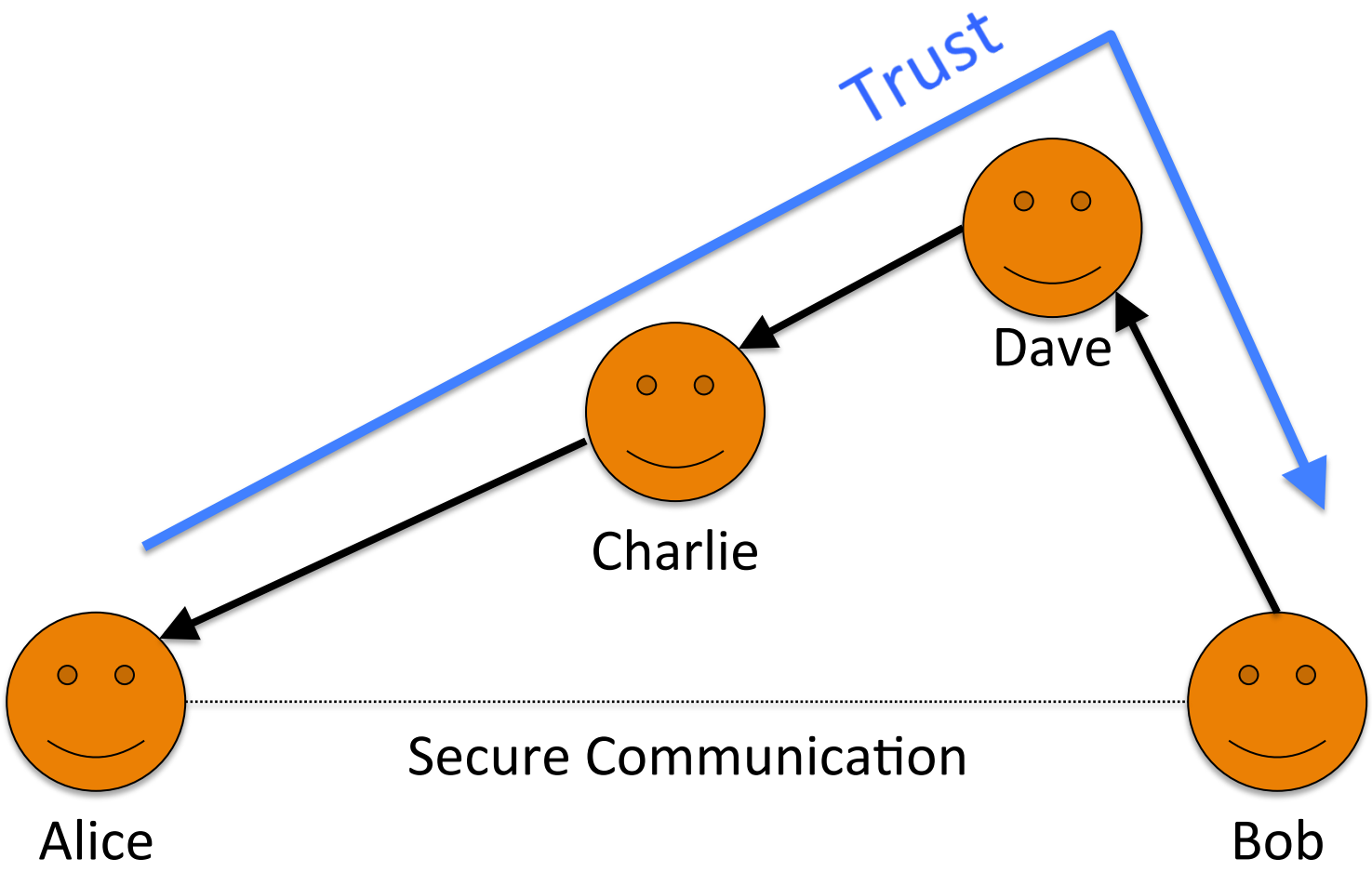
Web Presence



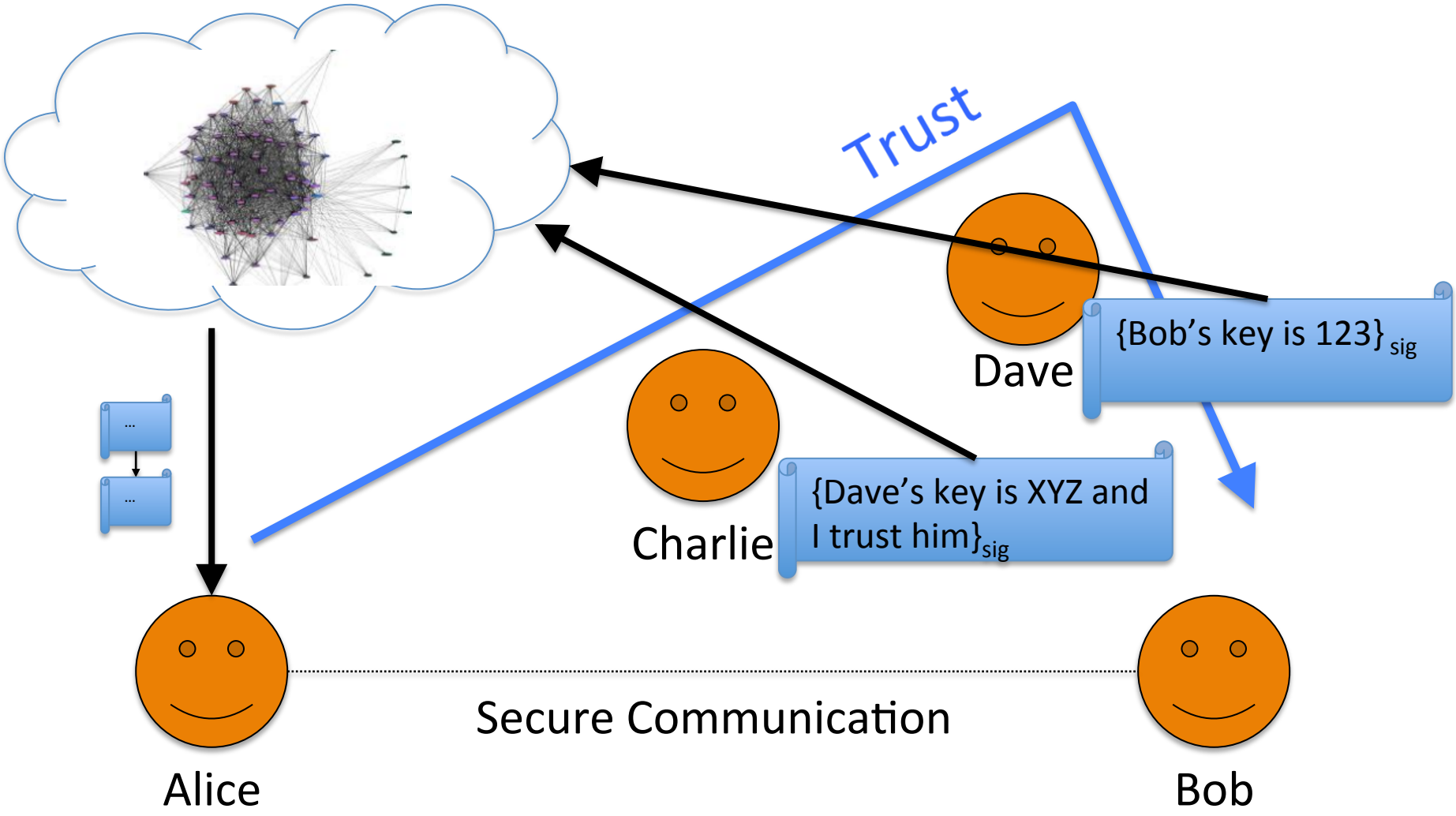
Person-to-Person

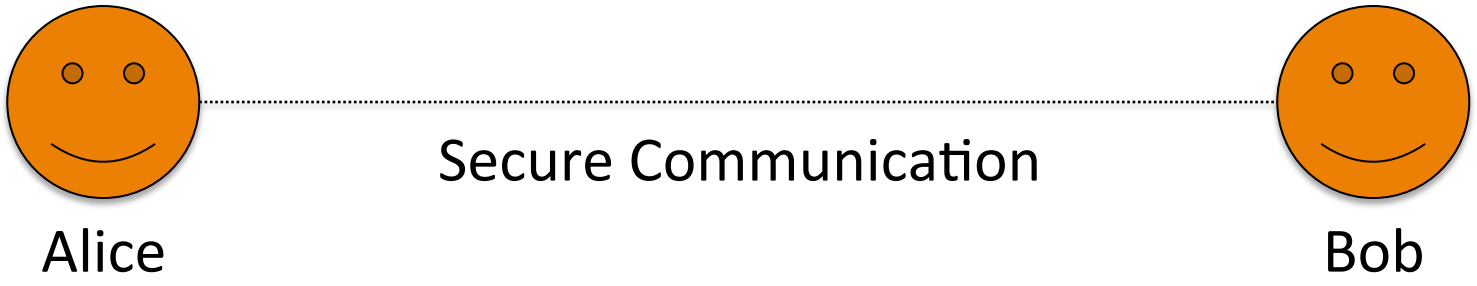


Web of Trust



Web of Trust


Trust
Dave
{Bob's key is 123}sig
Charlie
{Dave's key is XYZ and I trust him}sig
Alice
Secure Communication
Bob



- Asynchronous forward secrecy and integrity
- Group key management
- Group transcript consistency
- Multiple devices per user
- Anonymous message delivery
- High-latency mixes

Thanks!

- Lots of open questions for this contest and for UX research!

- Messaging mailing list
  - https://moderncrypto.org