

Interoperable Messaging

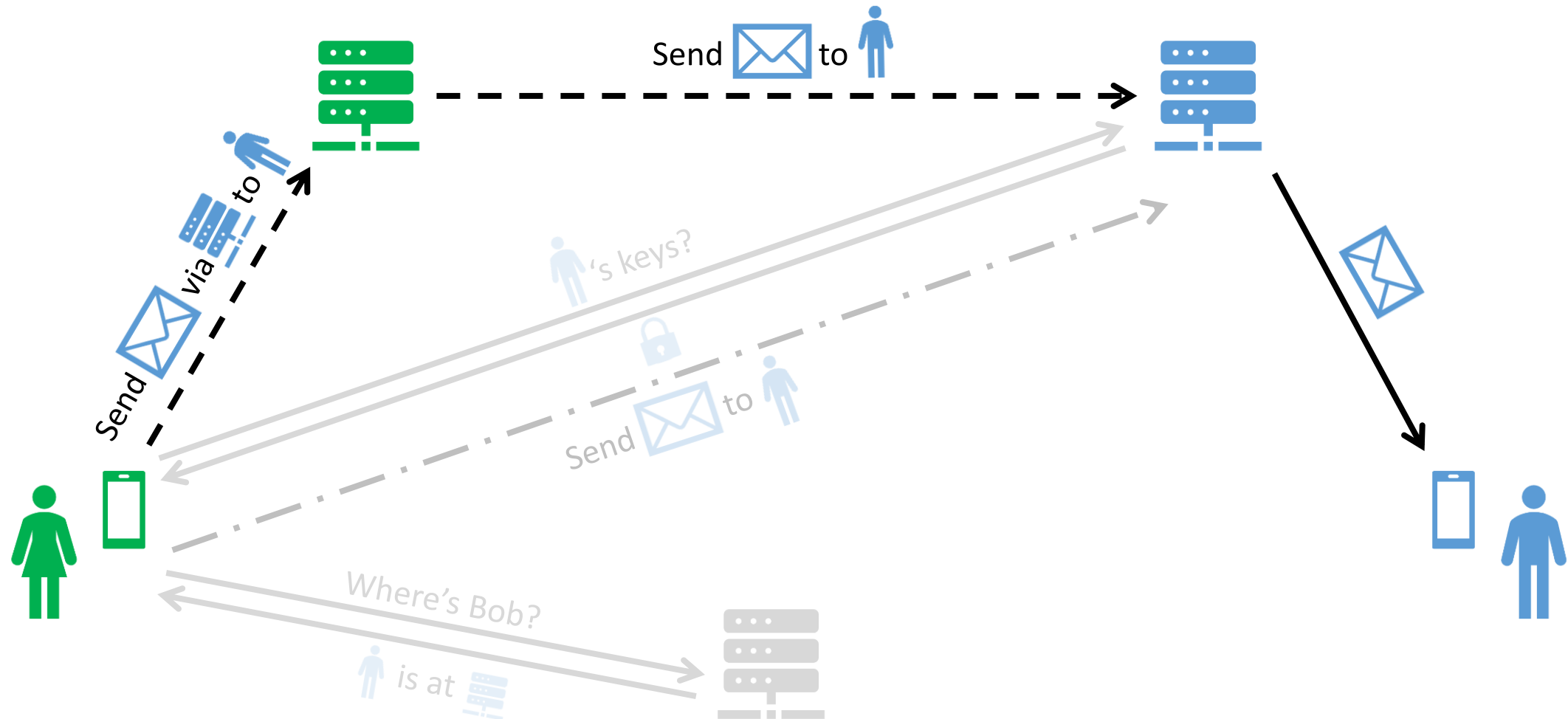
Panel 2: Secure Communication Protocol

23-02-28

Real-World Cryptography Group
FAU Erlangen-Nürnberg, Germany

Paul Rösler

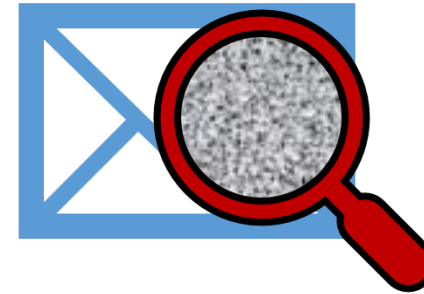
Overview of Setting



Requirements

End-to-End Confidentiality:

*“The **level of security**,
including the **end-to-end encryption**, [...] **shall be preserved** across the interoperable services.” §3*



Metadata Protection:

*“The gatekeeper shall **collect and exchange** [...] only the **personal data** of end users that is **strictly necessary** [...]” §8*



From:

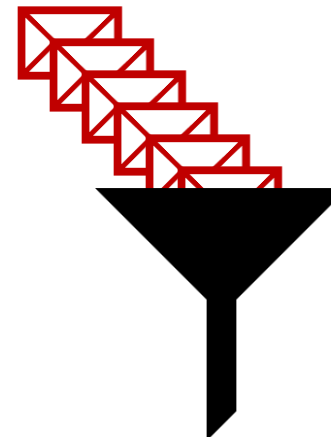


To:



Abuse Prevention:

*“The gatekeeper [should be able to **take**] **measures** to [...] **not endanger** the **integrity, security and privacy** of its services [...]” §9*



2. Standardization of Protocol

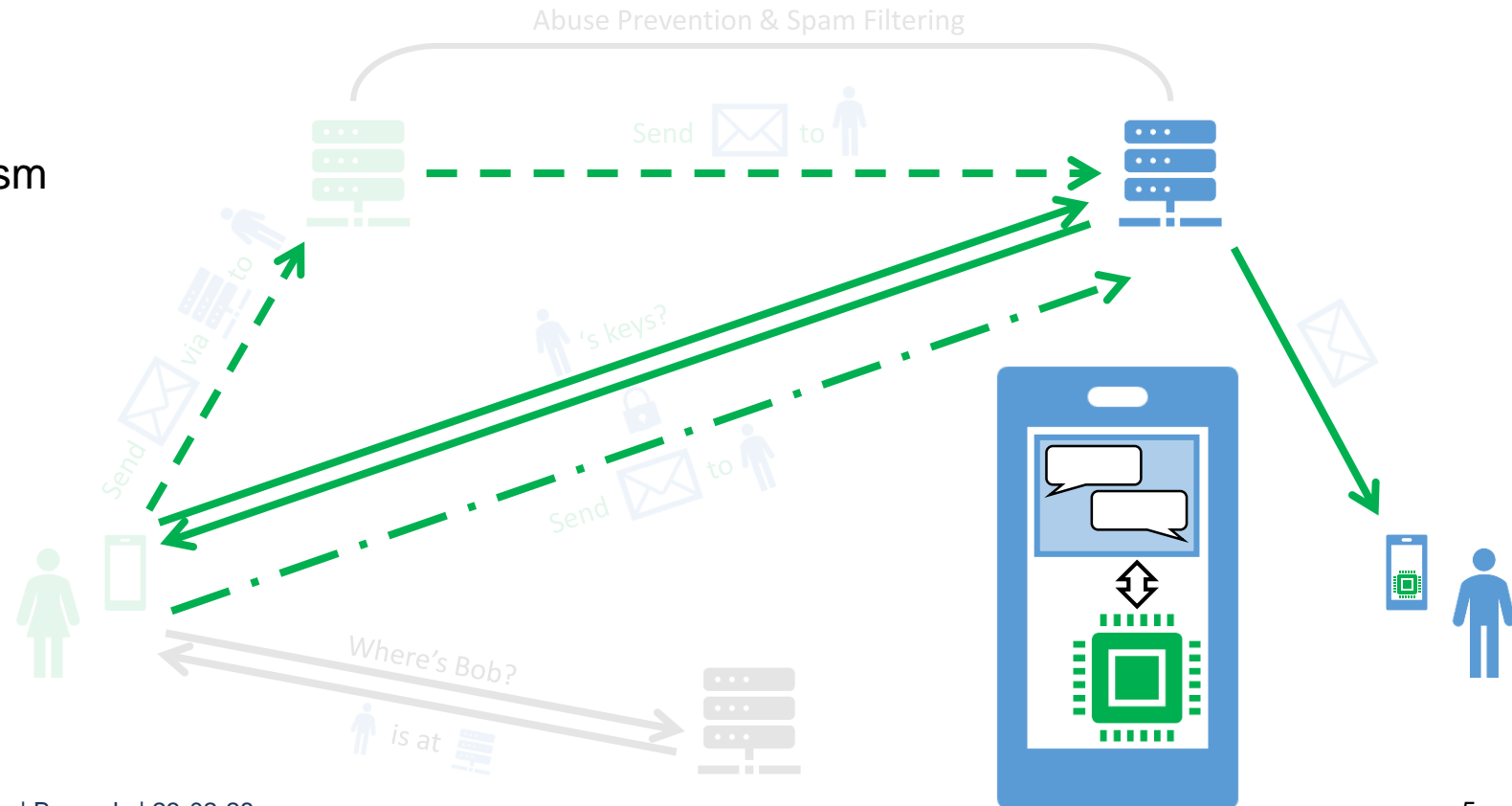
→ More in Alissa Cooper's talk

Communication Protocol

1. Gatekeeper's Core Protocol + X

- API + Documentation
- Client: Library?
- Server:
 - Replicate key distribution
 - Forwarding service
 - Abuse prevention (interactively)
 - Reporting and blocking mechanism

2. Standardization of Protocol

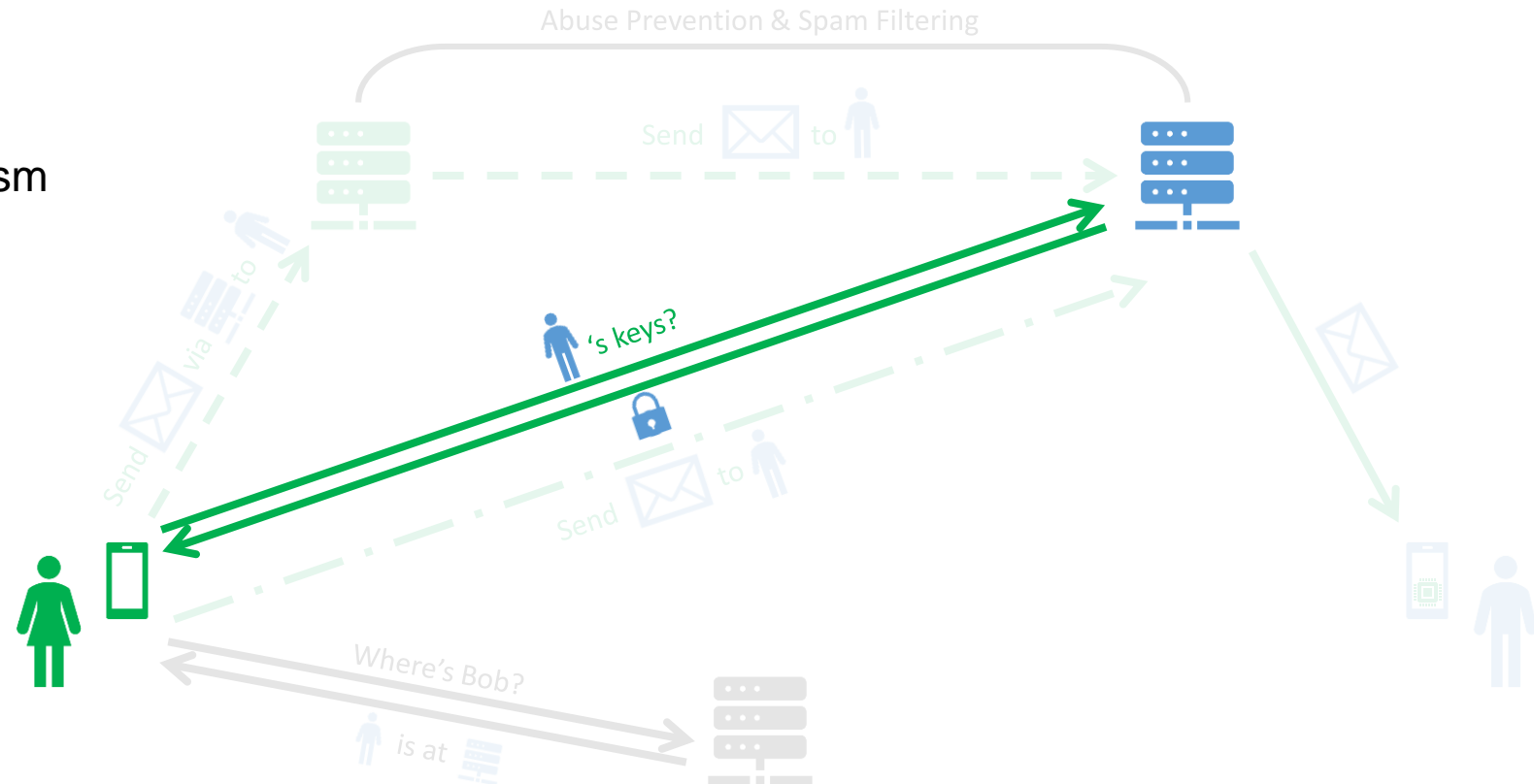


Communication Protocol

1. Gatekeeper's Core Protocol + X

- API + Documentation
- Client: Library?
- Server:
 - Replicate key distribution
 - Forwarding service
 - Abuse prevention (interactively)
 - Reporting and blocking mechanism

2. Standardization of Protocol

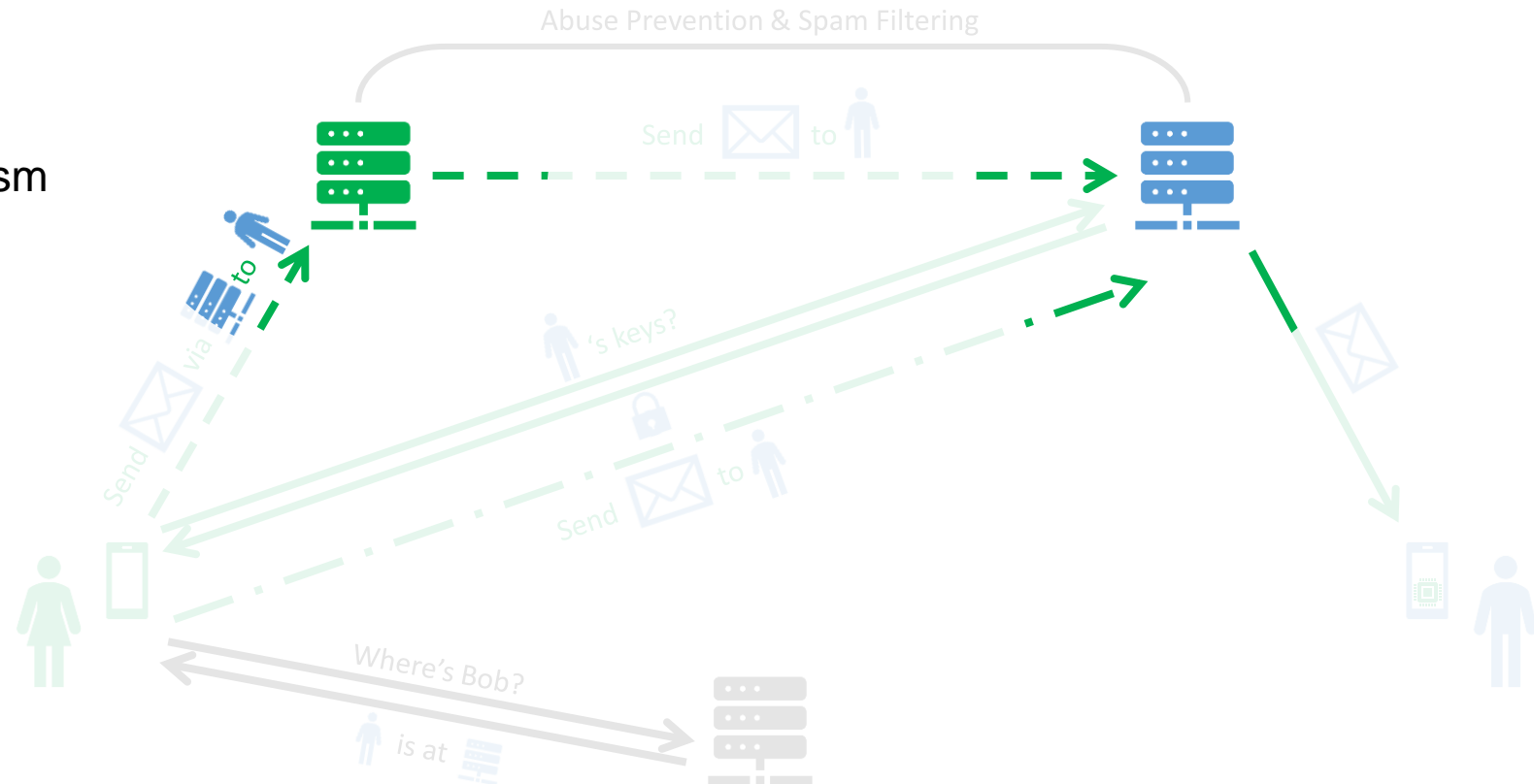


Communication Protocol

1. Gatekeeper's Core Protocol + X

- API + Documentation
- Client: Library?
- Server:
 - Replicate key distribution
 - Forwarding service
 - Abuse prevention (interactively)
 - Reporting and blocking mechanism

2. Standardization of Protocol



- API + Documentation
- Client: Library?
- Server:
 - Replicate key distribution
 - Forwarding service
 - Abuse prevention (interactively)
 - Reporting and blocking mechanism

[illegible]

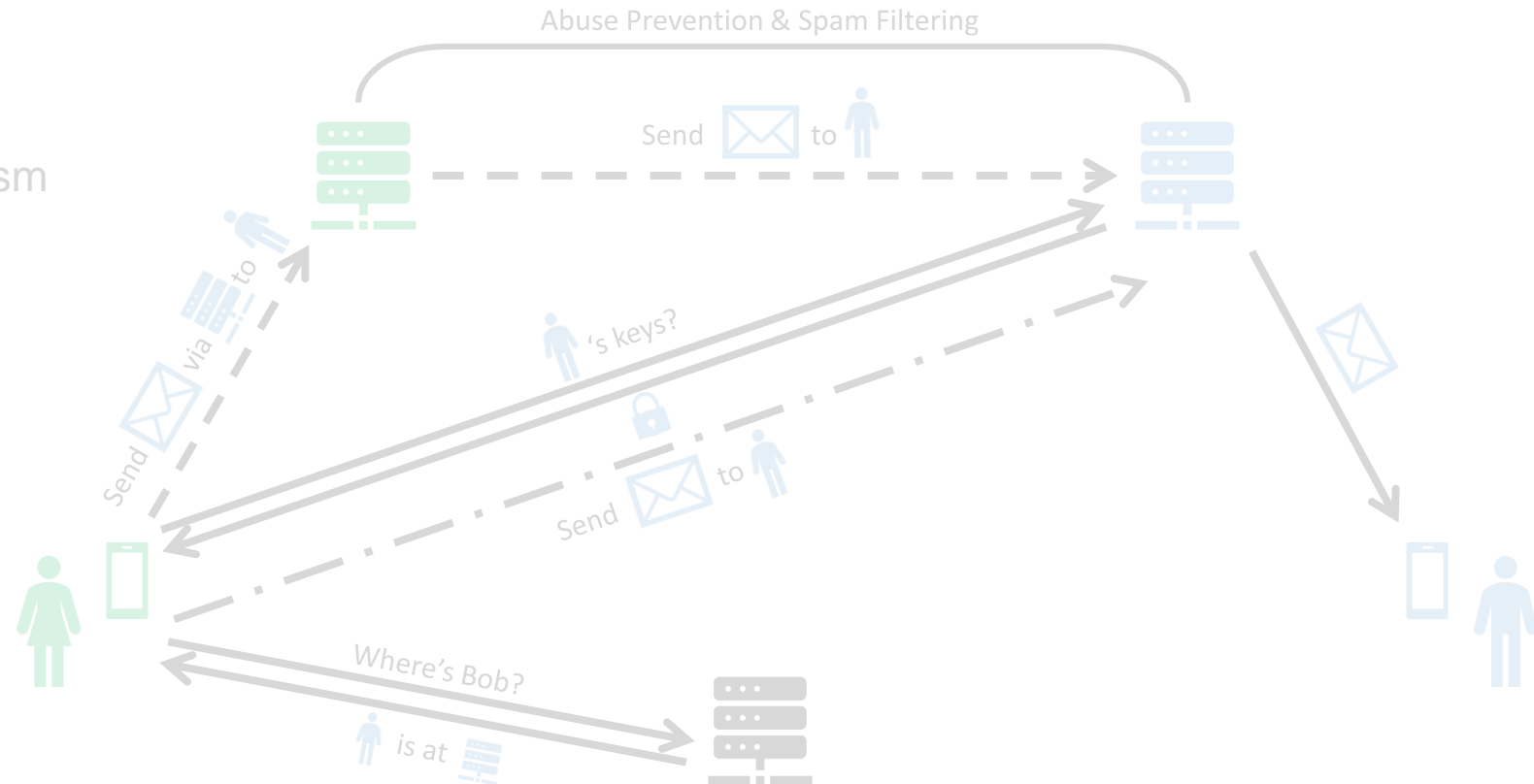
Communication Protocol

1. Gatekeeper's Core Protocol + X

- API + Documentation
- Client: Library?
- Server:
 - Replicate key distribution
 - Forwarding service
 - Abuse prevention (interactively)
 - Reporting and blocking mechanism

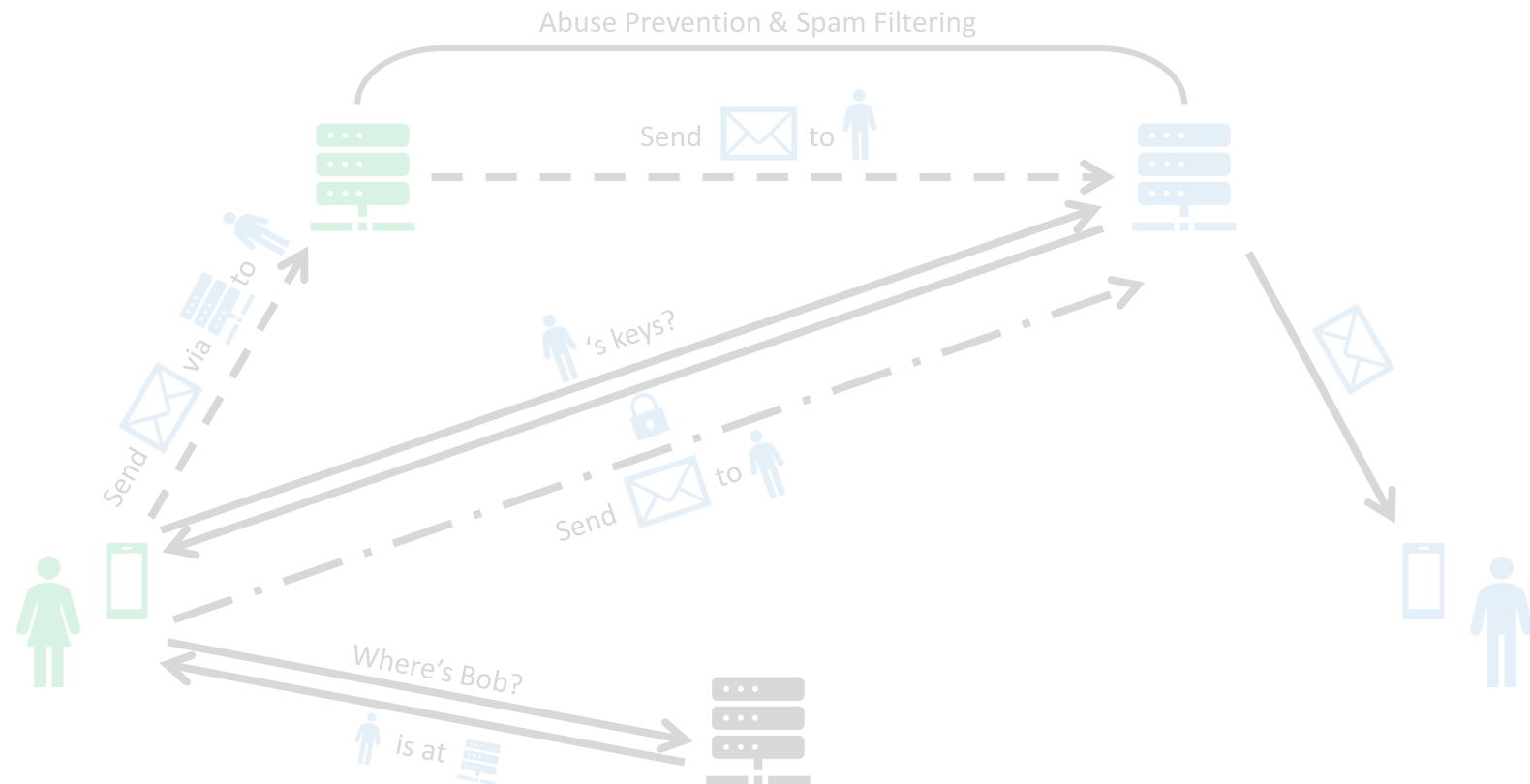
2. Standardization of Protocol

- New protocol
 - \geq Best gatekeeper
 - Simple standard update
 - Individual abuse prevention
- Don't start with solution



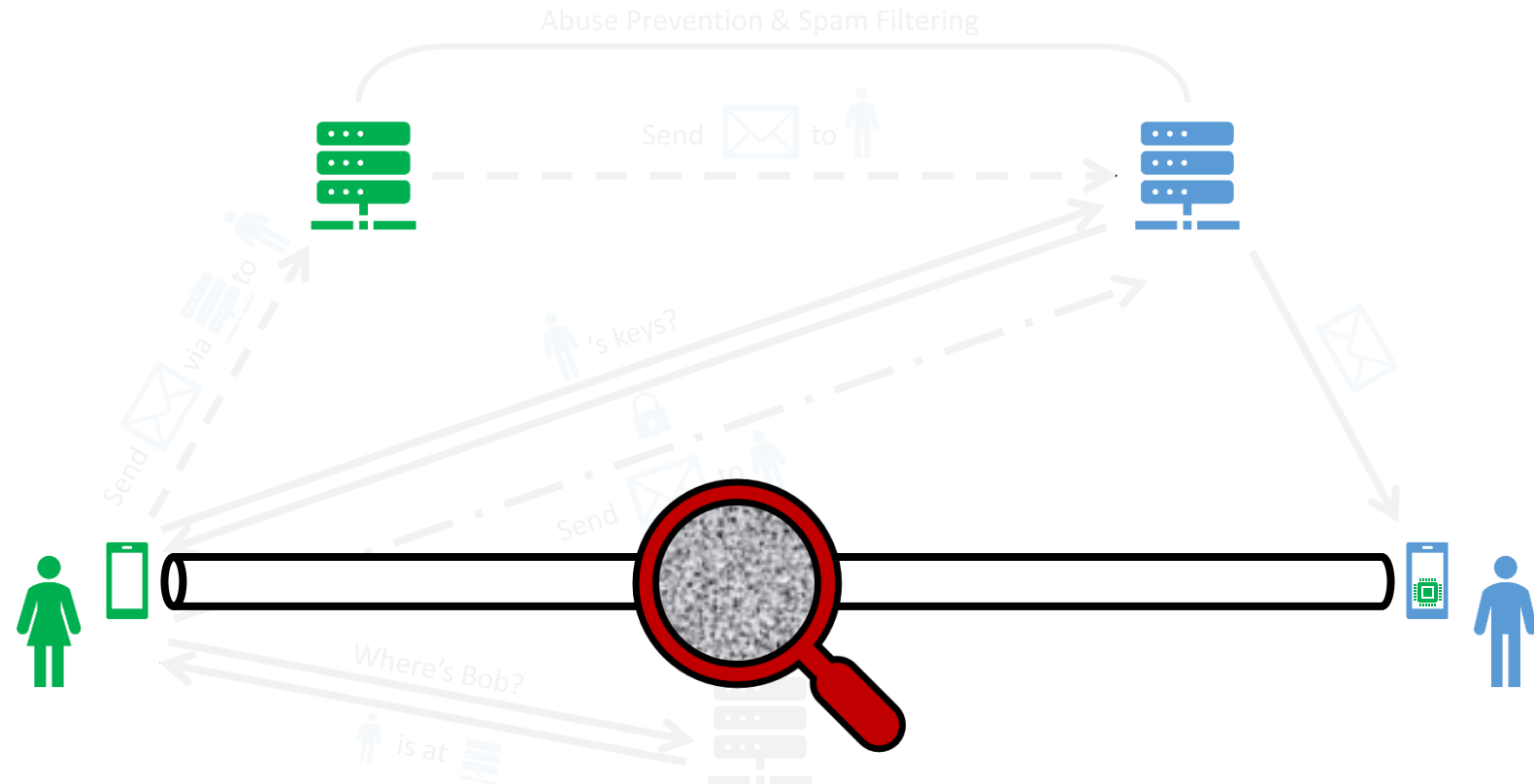
Confidentiality, Privacy & Abuse Prevention

Aka. “+ X”



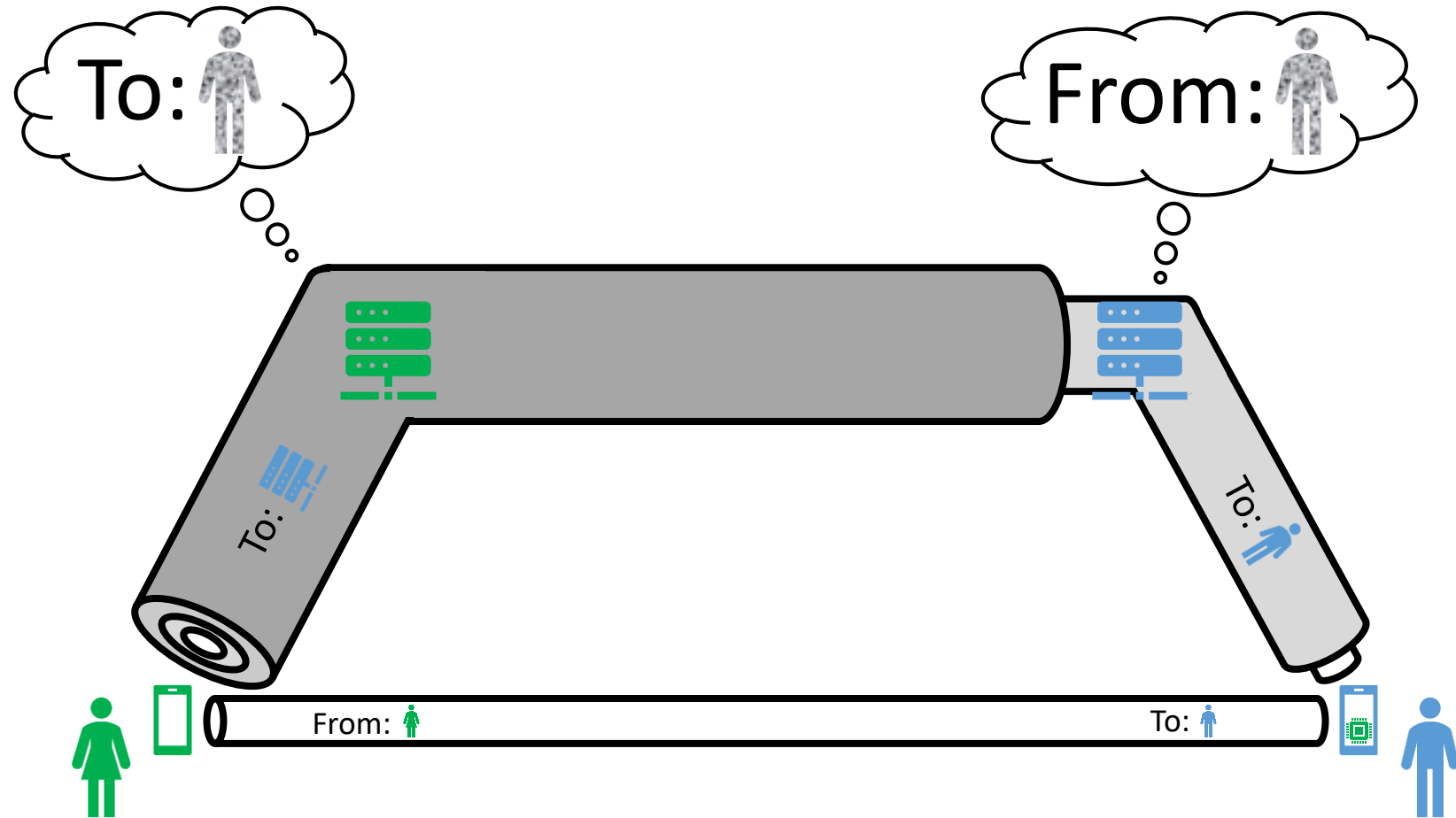
Confidentiality, Privacy & Abuse Prevention

- Message Delivery
 - Confidential + Y



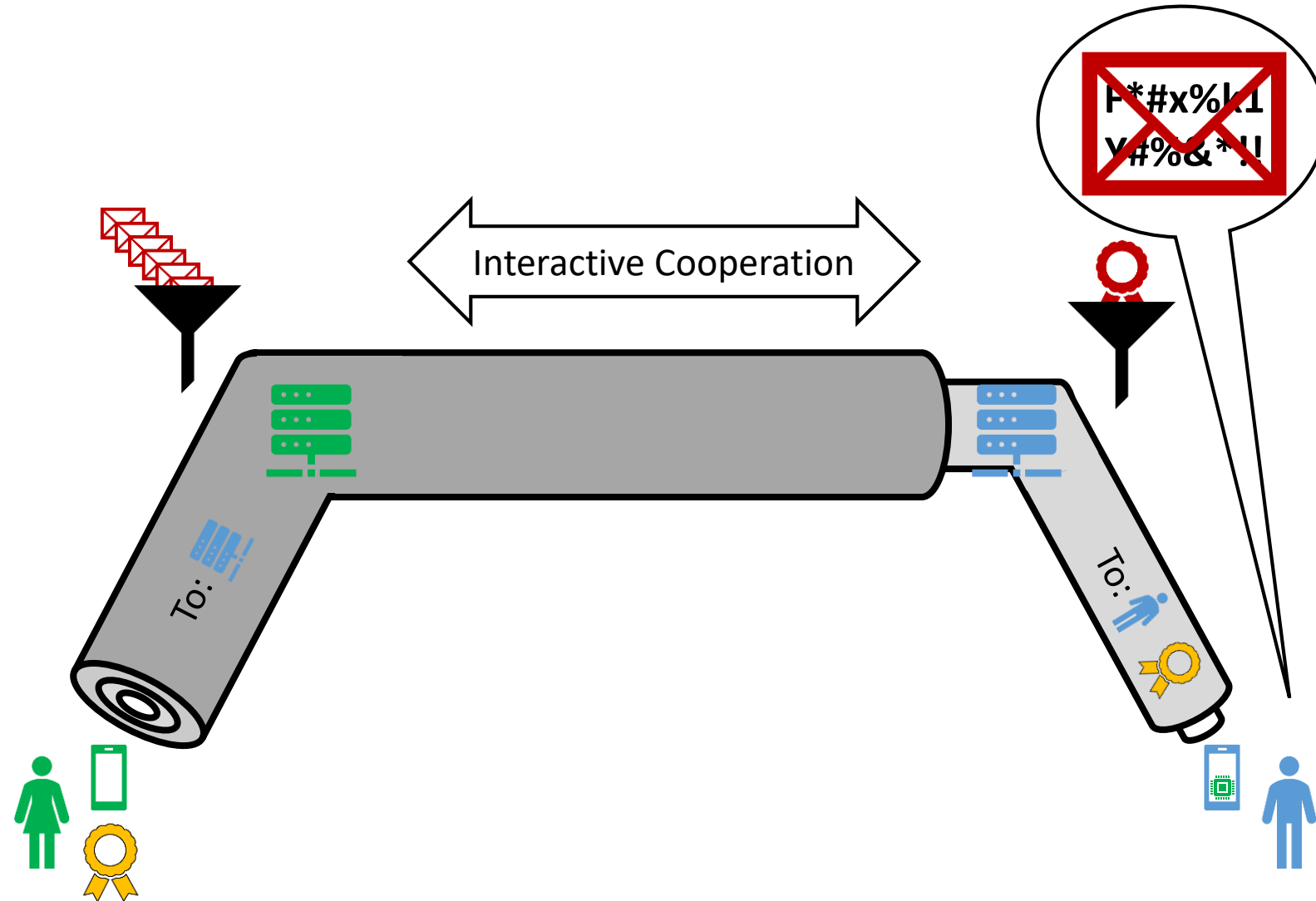
Confidentiality, Privacy & Abuse Prevention

- Message Delivery
 - Confidential + Y
 - Private



Confidentiality, Privacy & Abuse Prevention

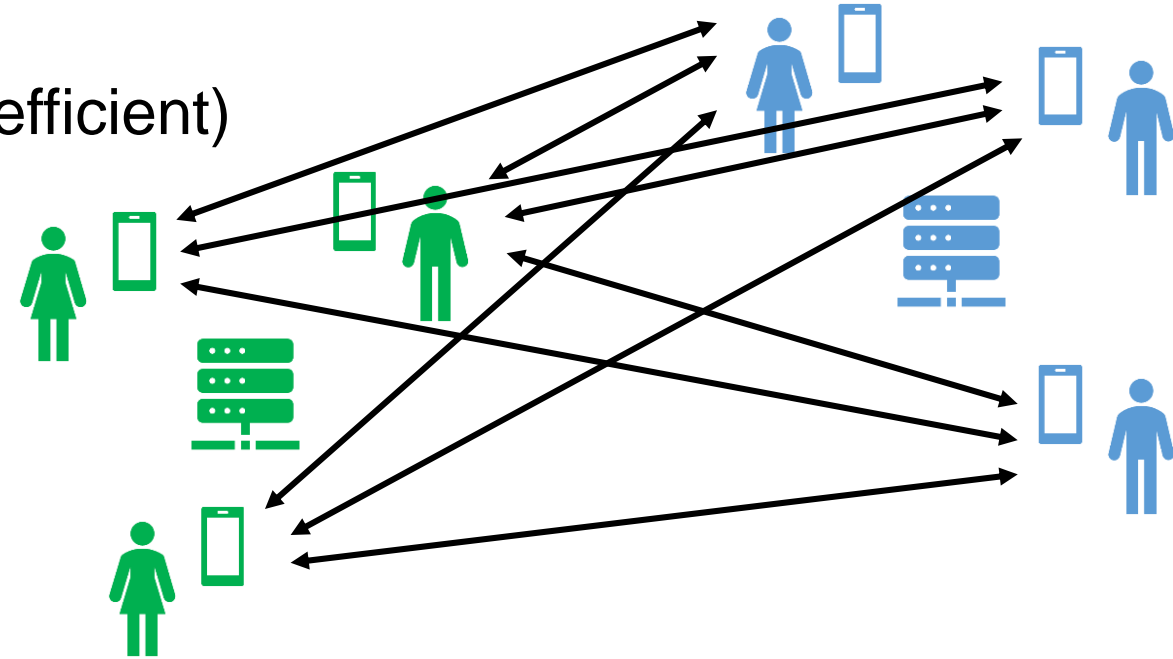
- Message Delivery
 - Confidential + Y
 - Private
- Abuse Reporting
- Effective User Blocking
 - For Individuals
 - From Platform
- Spam Filtering



Group Messaging

Alternatives:

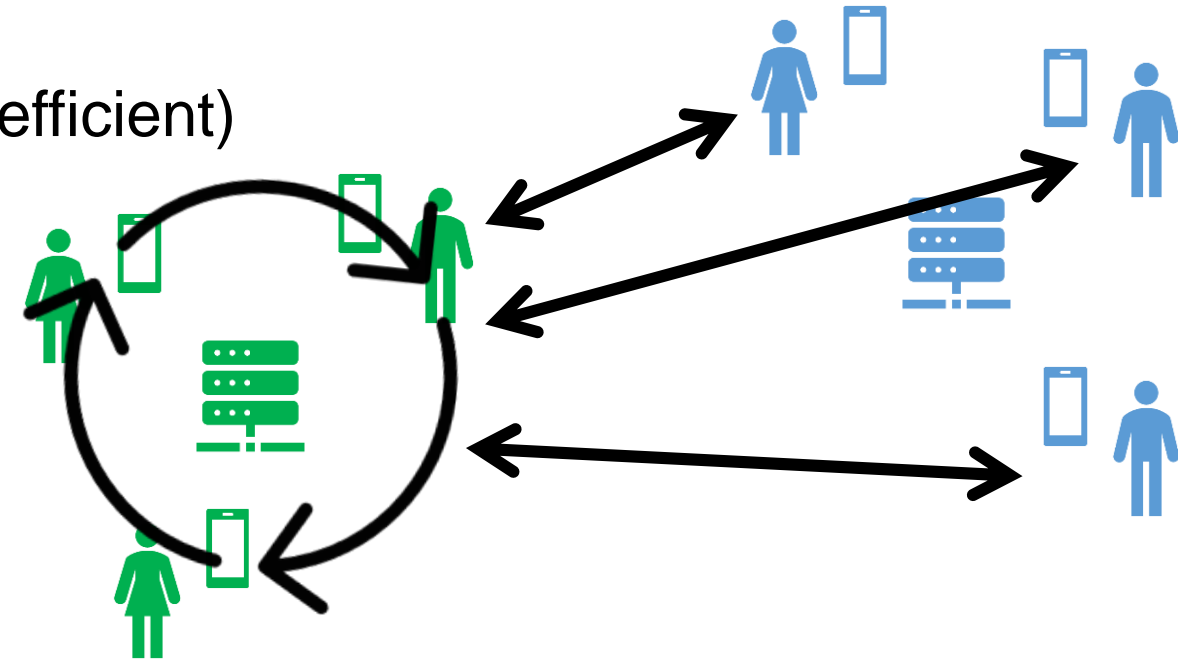
1. Via Pair-Wise Channels (Simple but Inefficient)
2. Gatekeeper's Core Protocol
3. Connect Providers' Subgroups
4. Standardize Group Protocol



Group Messaging

Alternatives:

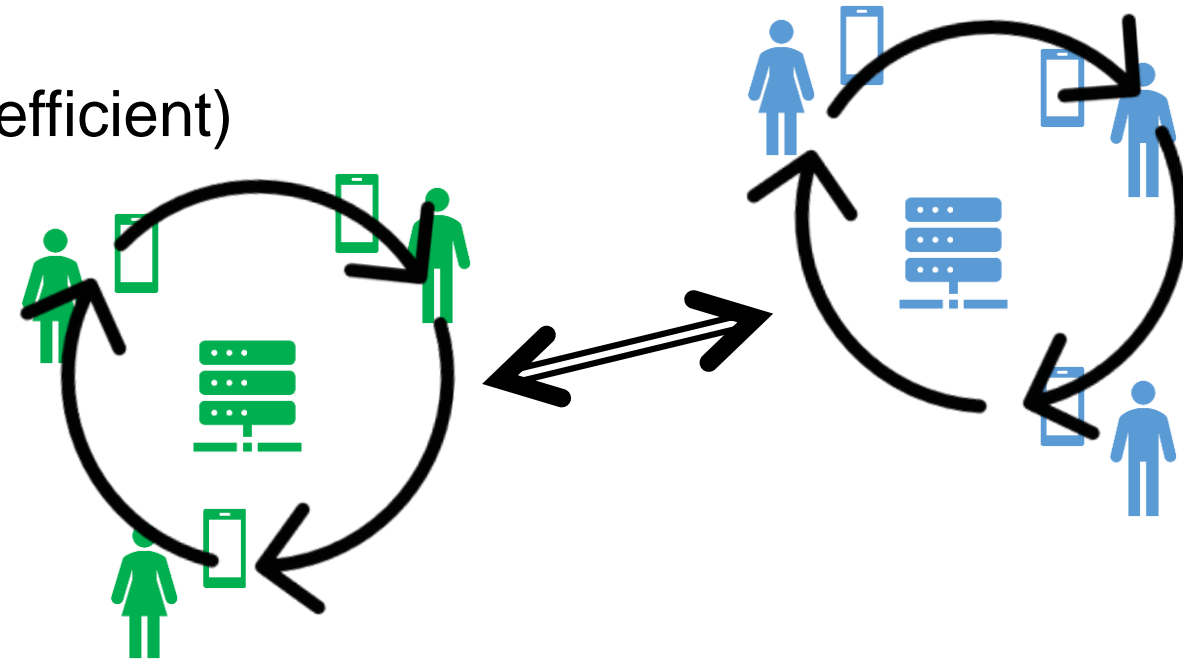
1. Via Pair-Wise Channels (Simple but Inefficient)
2. Gatekeeper's Core Protocol
3. Connect Providers' Subgroups
4. Standardize Group Protocol



Group Messaging

Alternatives:

1. Via Pair-Wise Channels (Simple but Inefficient)
2. Gatekeeper's Core Protocol
3. Connect Providers' Subgroups
4. Standardize Group Protocol



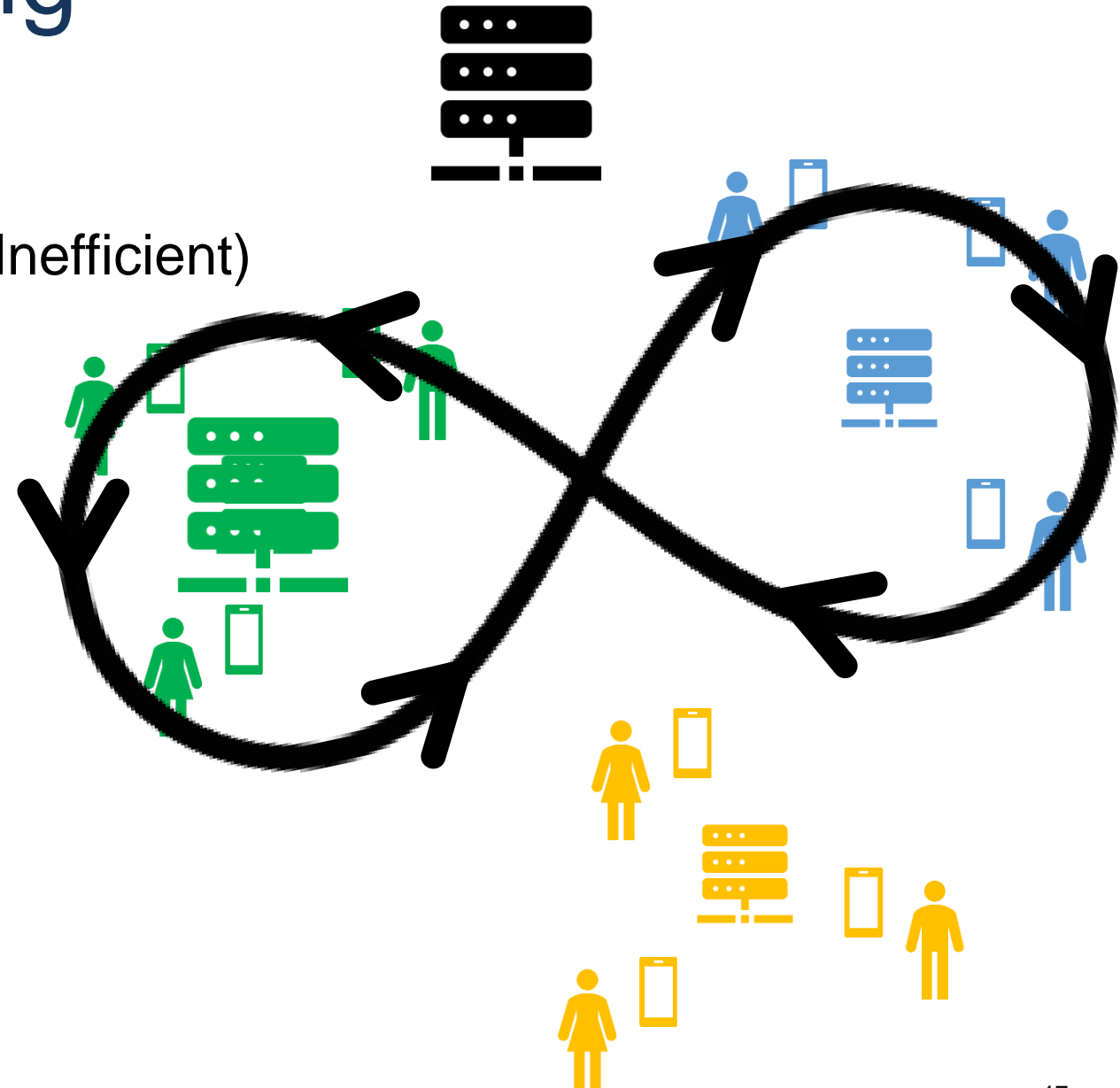
Group Messaging

Alternatives:

1. Via Pair-Wise Channels (Simple but Inefficient)
2. Gatekeeper's Core Protocol
3. Connect Providers' Subgroups
4. Standardize Group Protocol

Problems and Solutions:

- Consistent Group Management:
 - Centralized?
 - Where?
- Multiple Gatekeepers & Non-Gatekeepers



Conclusion

- Confidentiality, Privacy & Abuse Prevention:
 - Required!
 - Practical ✓
- Gatekeeper's vs. Standard Protocol
 - Tradeoffs:
 - Replication & Implementation Overhead
 - Standardization Overhead
 - Agility
 - Group Efficiency
- Standard Tools Deployed

Interoperability in End-to-End Encrypted Messaging

Julia Len, Esha Ghosh, Paul Grubbs, Paul Rösler
Cornell Tech, Microsoft Research, University of Michigan, FAU Erlangen-Nürnberg

Thank you!

Questions & Comments?

paul.roesler@fau.de

@roeslpa