# Interoperability in E2EE Messaging


Julia Len
Cornell Tech
jlen@cs.cornell.edu

Paul Grubbs
University of Michigan
paulgrub@umich.edu

Esha Ghosh
Microsoft Research
esha.ghosh@microsoft.com

Paul Rösler
FAU Erlangen-Nürnberg
paul.roesler@fau.de



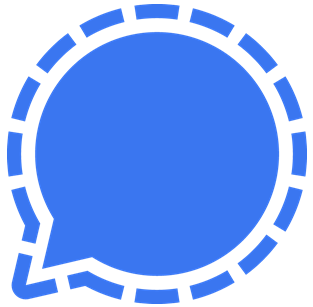
Real World Crypto 2023
March 28, 2023

# End-to-End Encrypted Messaging Today

# End-to-End Encrypted Messaging Today


Telegram

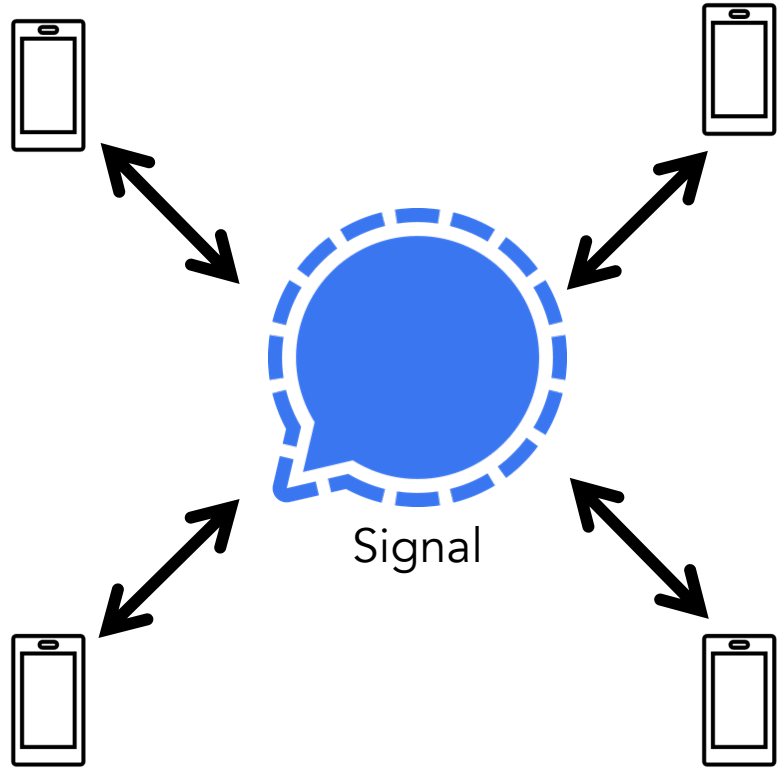

WhatsApp


Signal


iMessage


Google Messages

# End-to-End Encrypted Messaging Today

# End-to-End Encrypted Messaging Today

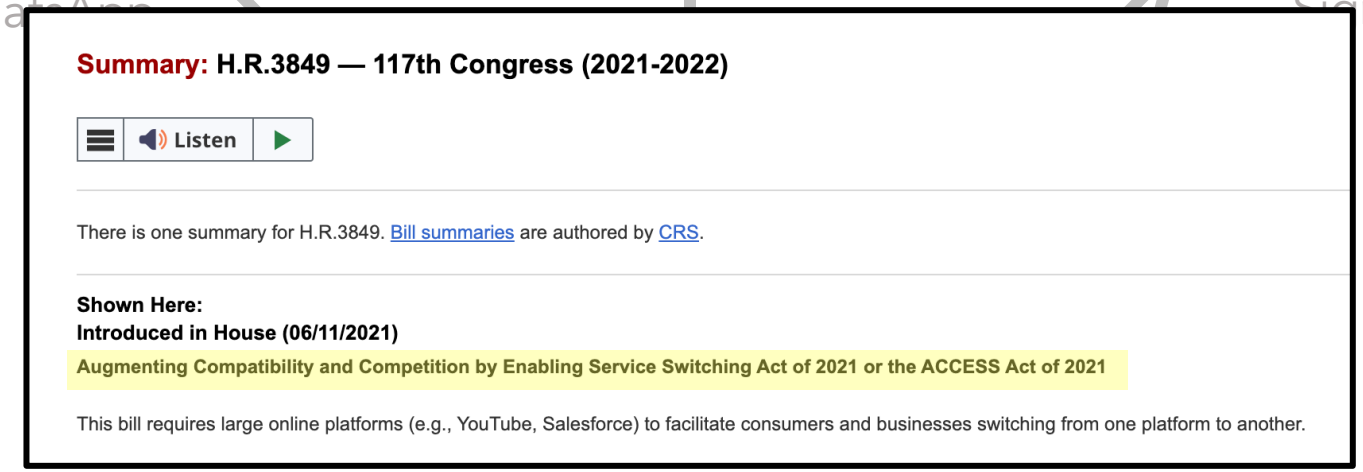

In September 2022, the E.U. signed the Digital Markets Act (DMA) into law.

- Goal: reduce network effects of large messaging apps
- Includes interoperability mandate for large “gatekeeper” E2EE messaging apps

# End-to-End Encrypted Messaging Today

In September 2022, the E.U. signed the Digital Markets Act (DMA) into law.

- Goal: reduce network effects of large messaging apps
- Includes interoperability mandate for large "gatekeeper" E2EE messaging apps



**Summary:** H.R.3849 — 117th Congress (2021-2022)

Listen

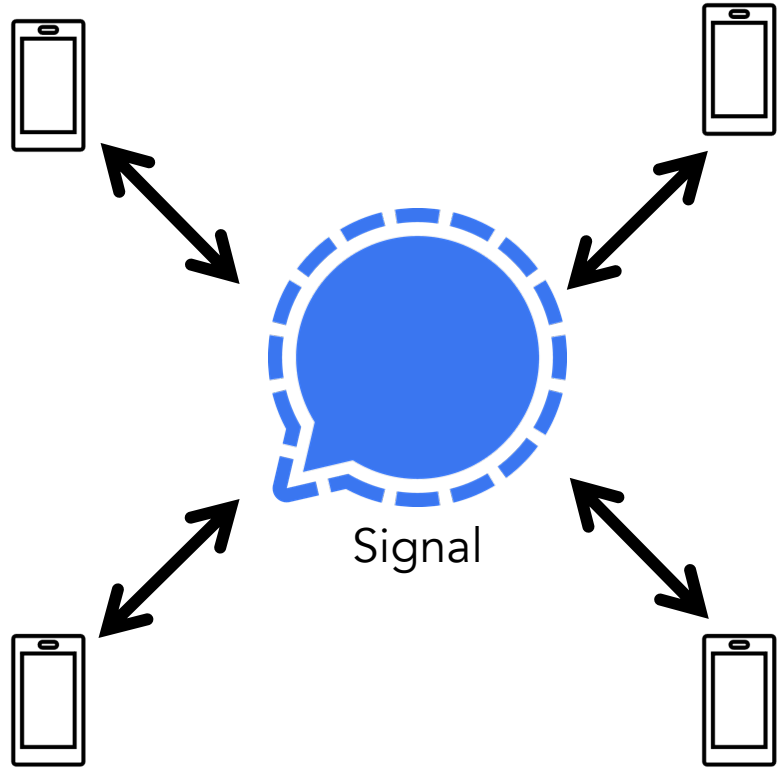
There is one summary for H.R.3849. Bill summaries are authored by CRS.

**Shown Here:**
**Introduced in House (06/11/2021)**

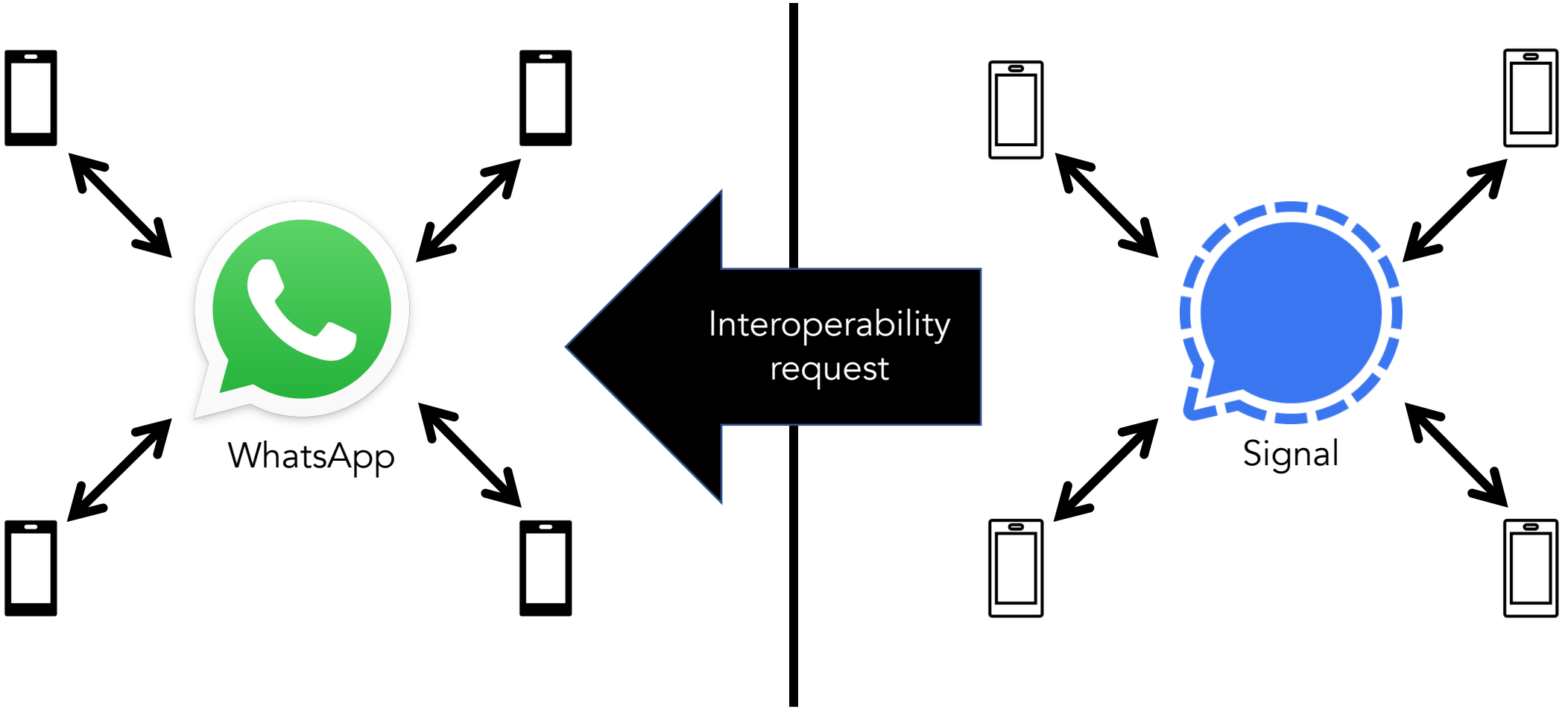
**Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021 or the ACCESS Act of 2021**

This bill requires large online platforms (e.g., YouTube, Salesforce) to facilitate consumers and businesses switching from one platform to another.

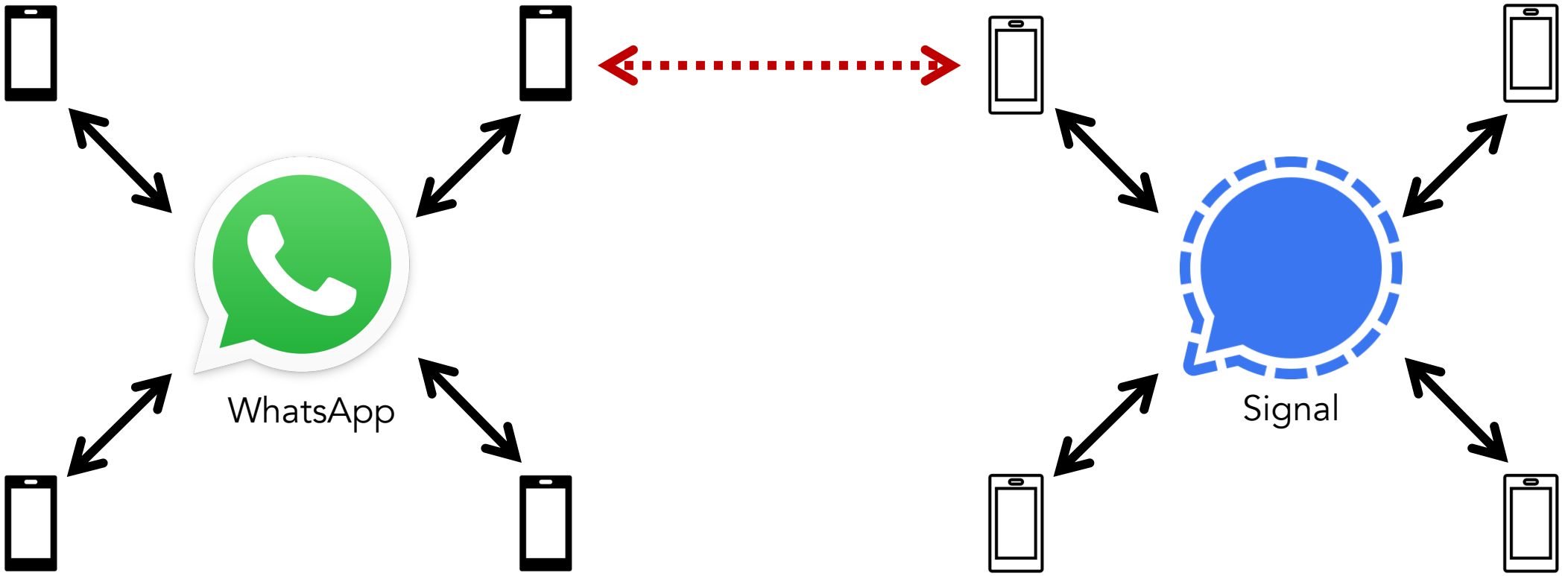
# End-to-End Encrypted Messaging Today

# End-to-End Encrypted Messaging Today

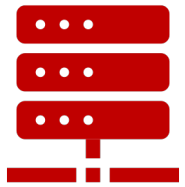


# End-to-End Encrypted Messaging Today

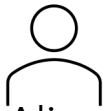


# End-to-End Encrypted Messaging Today

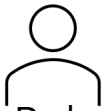
# New Challenges



Service Provider 1

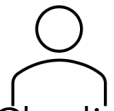


Alice

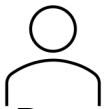


Bob

Service Provider 2

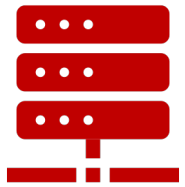


Charlie



Dan

# New Challenges



Service Provider 1

Alice

(111)111-1111

Bob

(222)222-2222

Phone numbers as user identifiers

Service Provider 2

Charlie

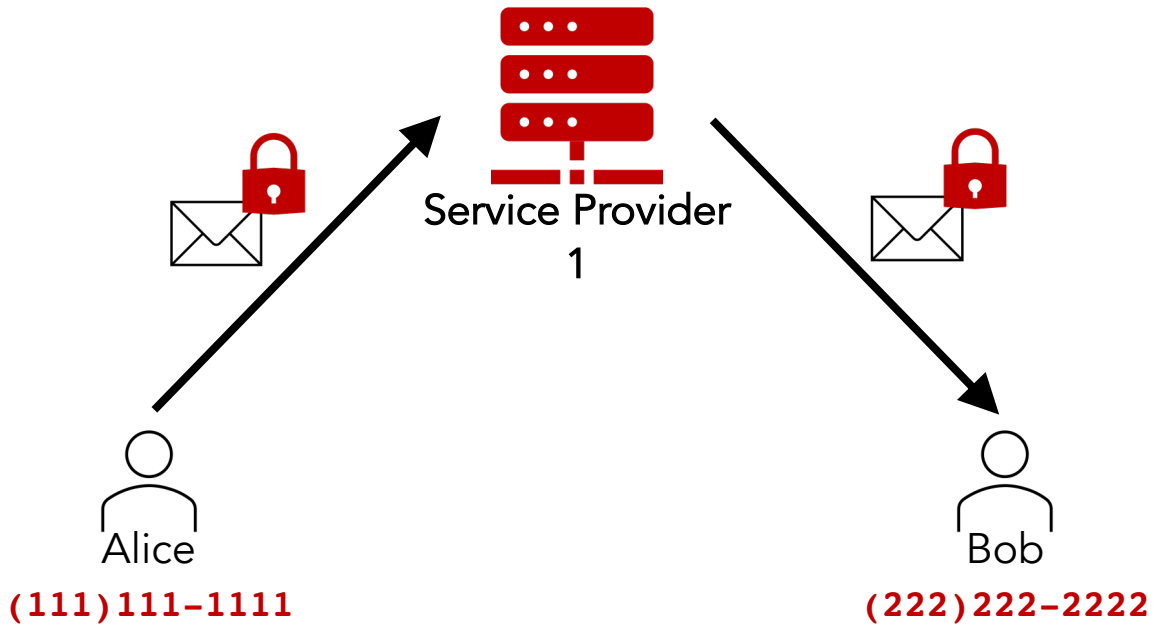
charlie@email.com

Dan

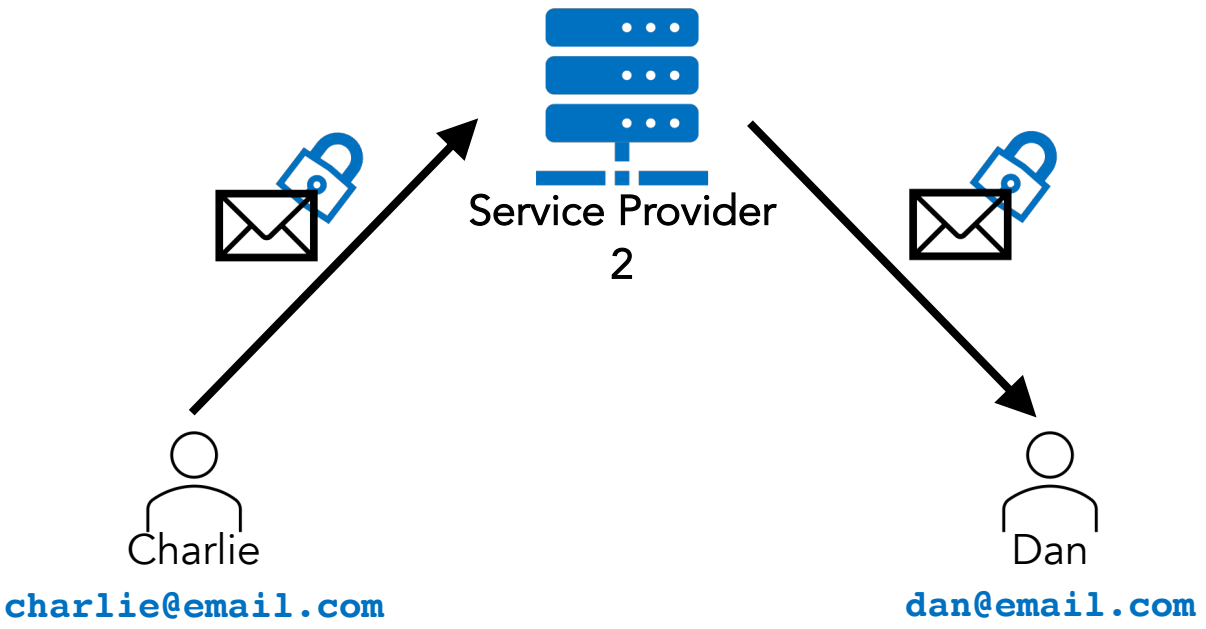
dan@email.com

Email as user identifiers

# New Challenges

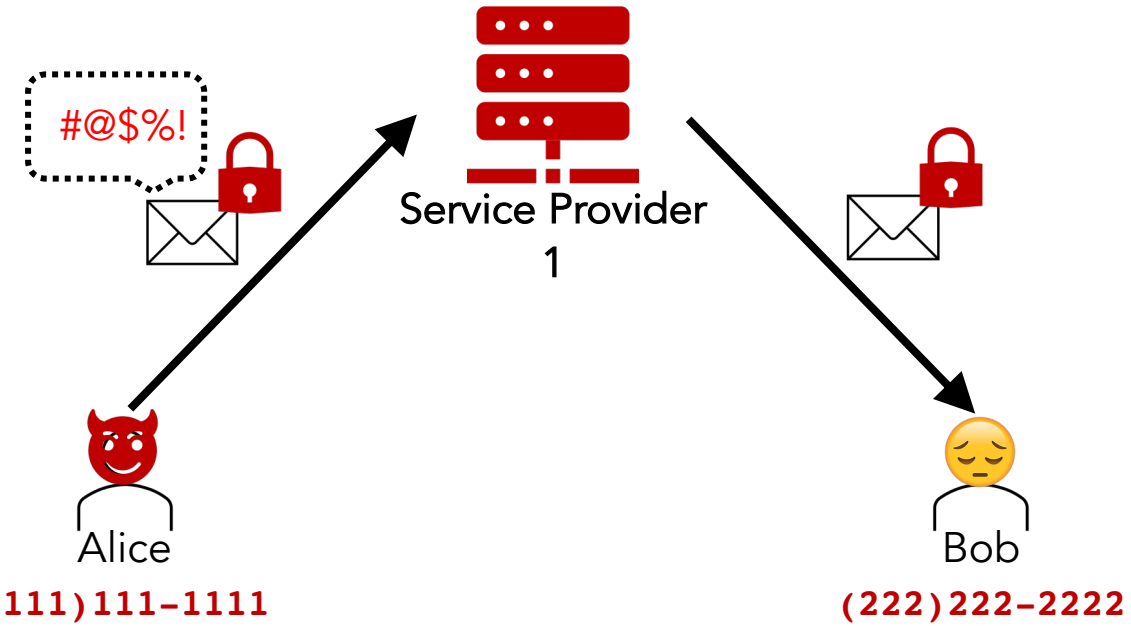



Uses Signal's Double Ratchet algorithm for E2EE protocol

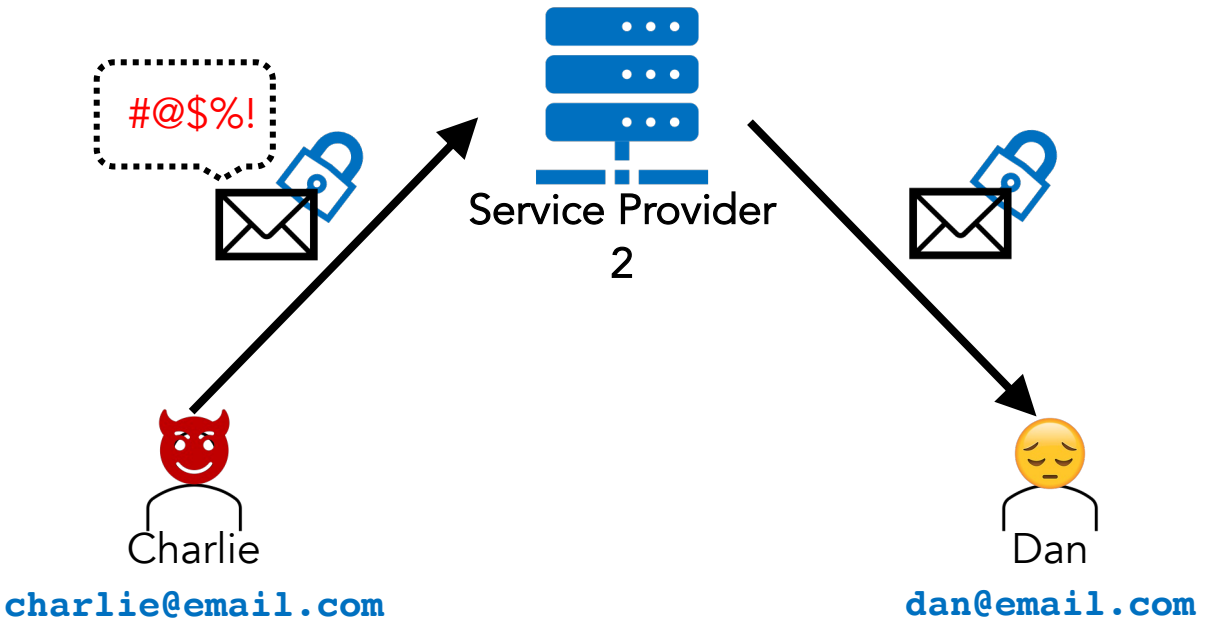



Uses MTProto algorithm for E2EE protocol

# New Challenges

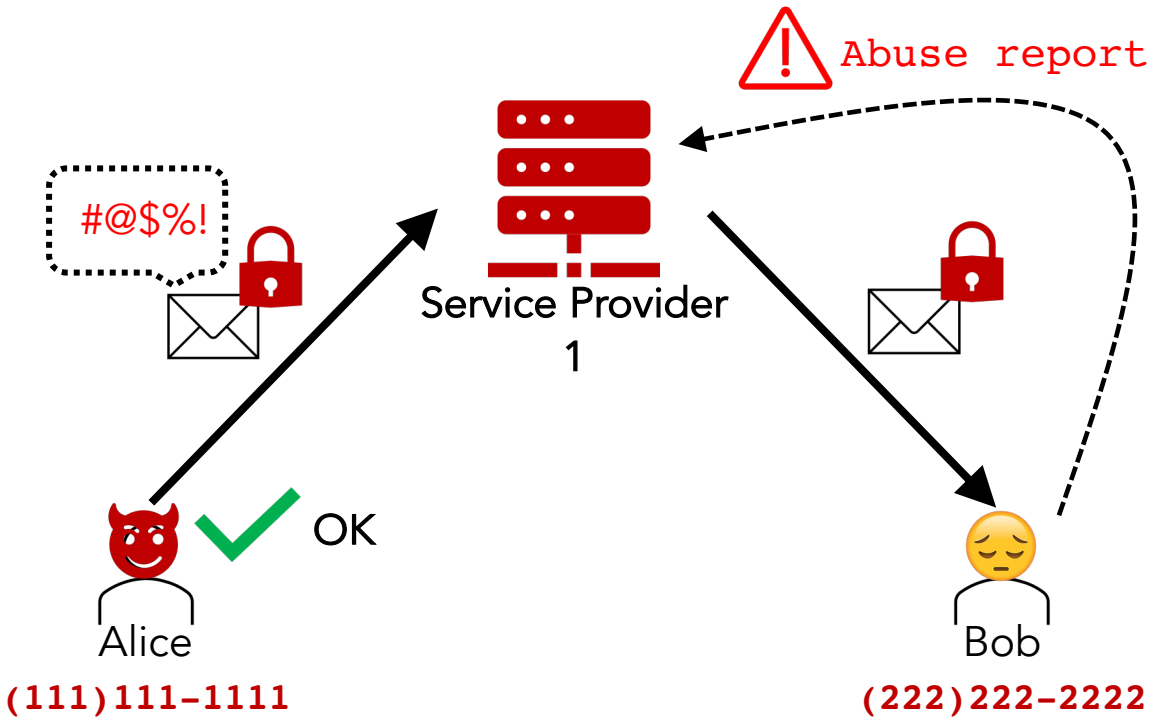



Alice's behavior *does not* violate Terms of Service for Provider 1

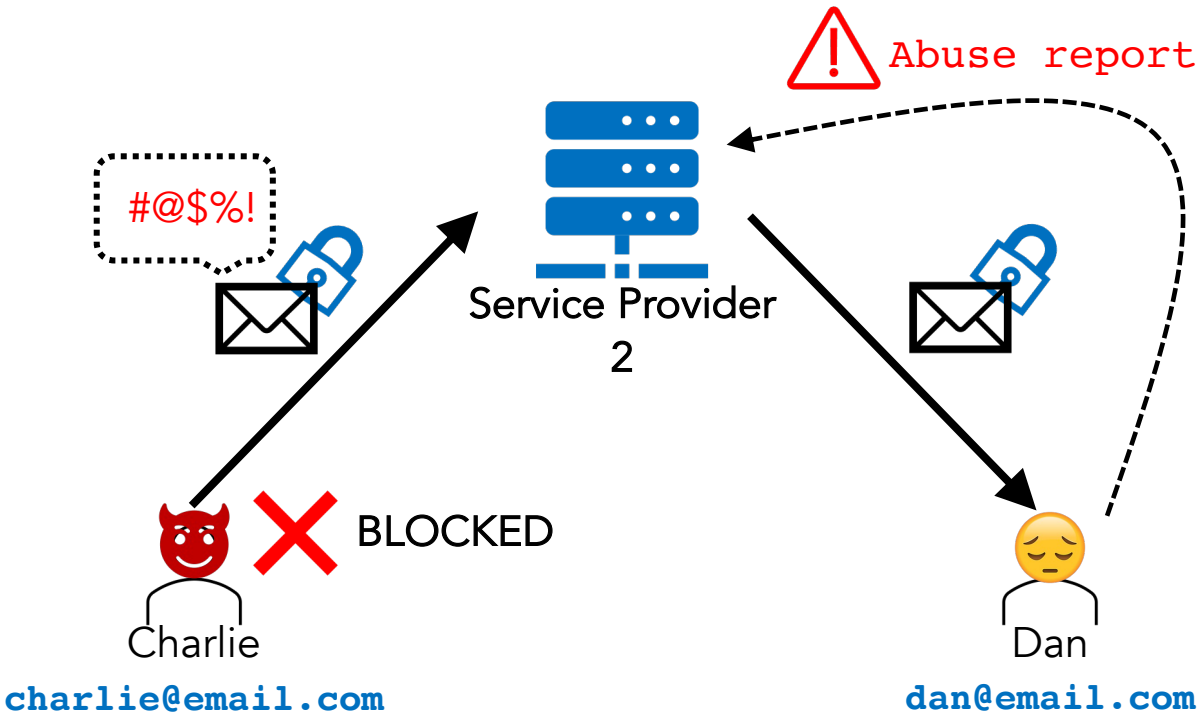



Charlie's behavior *does* violate Terms of Service for Provider 2

# New Challenges

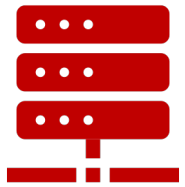



Alice's behavior *does not* violate Terms of Service for Provider 1

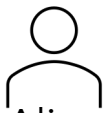



Charlie's behavior *does* violate Terms of Service for Provider 2

# New Challenges

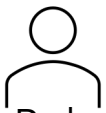


Service Provider 1



Alice

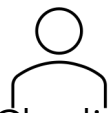
(111)111-1111



Bob

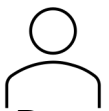
(222)222-2222

Service Provider 2



Charlie

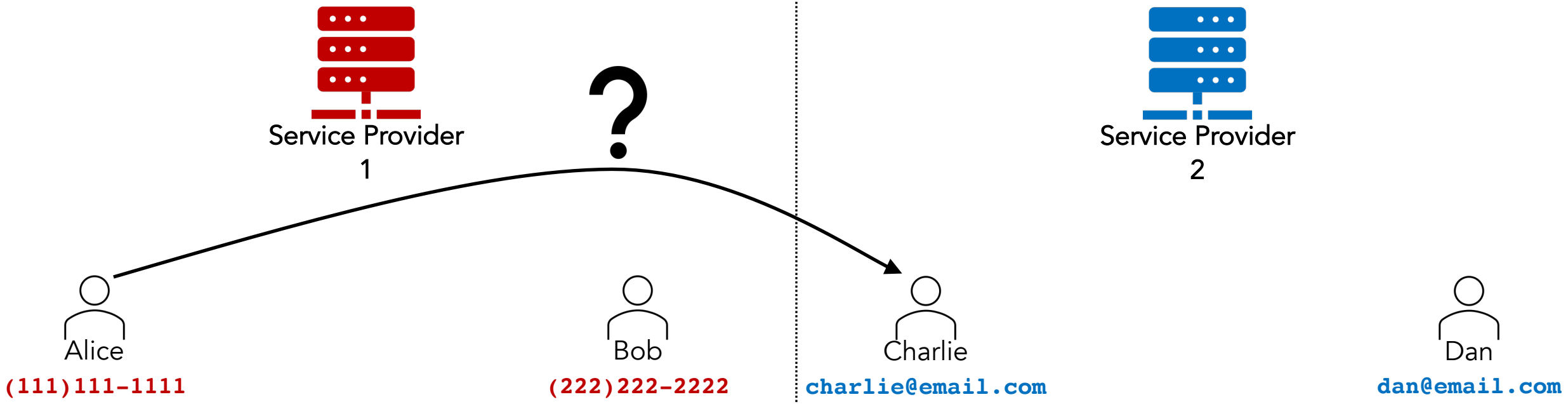
charlie@email.com



Dan

dan@email.com

# New Challenges



# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

Disclaimer: We are not lawyers or legal experts

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

Disclaimer: We are not lawyers or legal experts

Three components of messaging affected by the DMA:

1) Identity systems
2) E2EE protocols
3) Abuse prevention

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

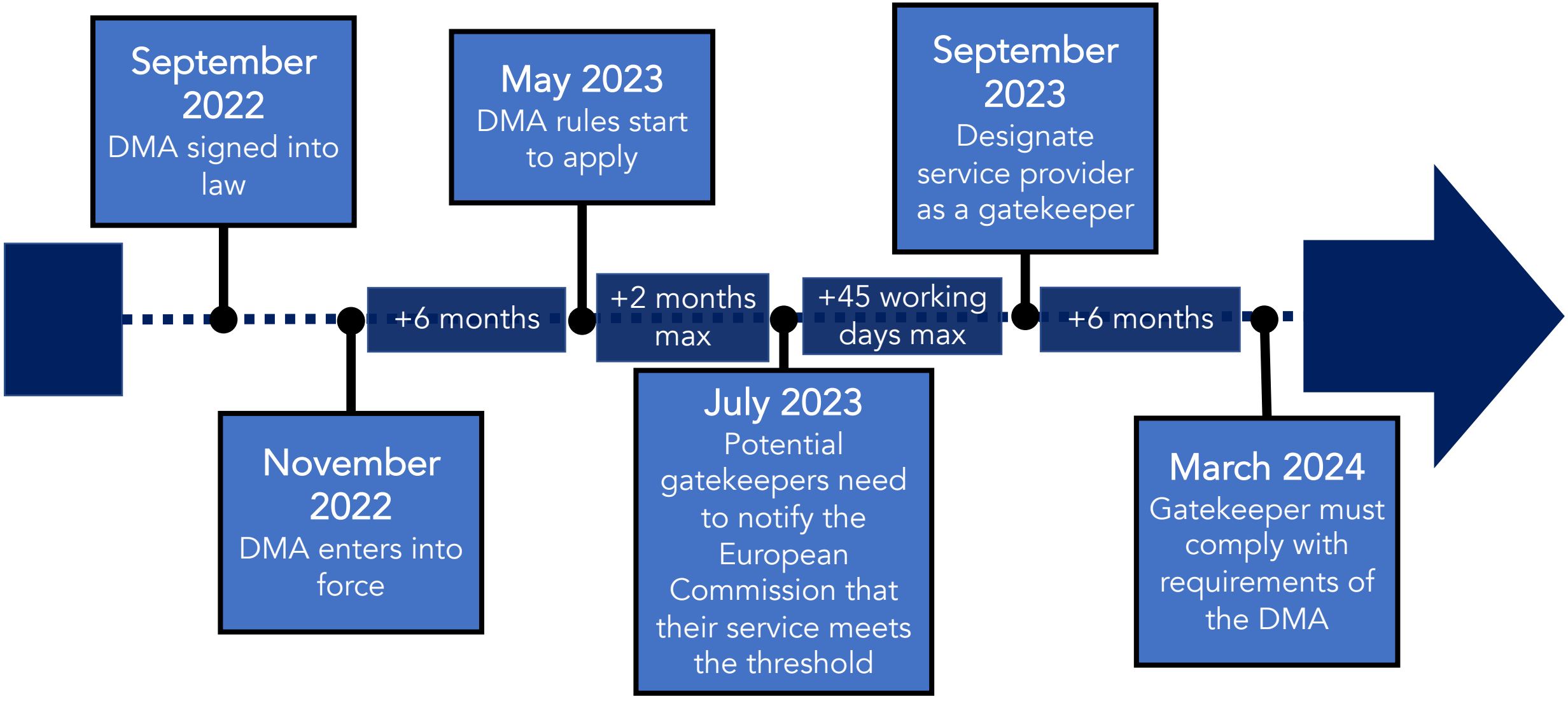
Disclaimer: We are not lawyers or legal experts

Three components of messaging affected by the DMA:

1) Identity systems
2) E2EE protocols
3) Abuse prevention

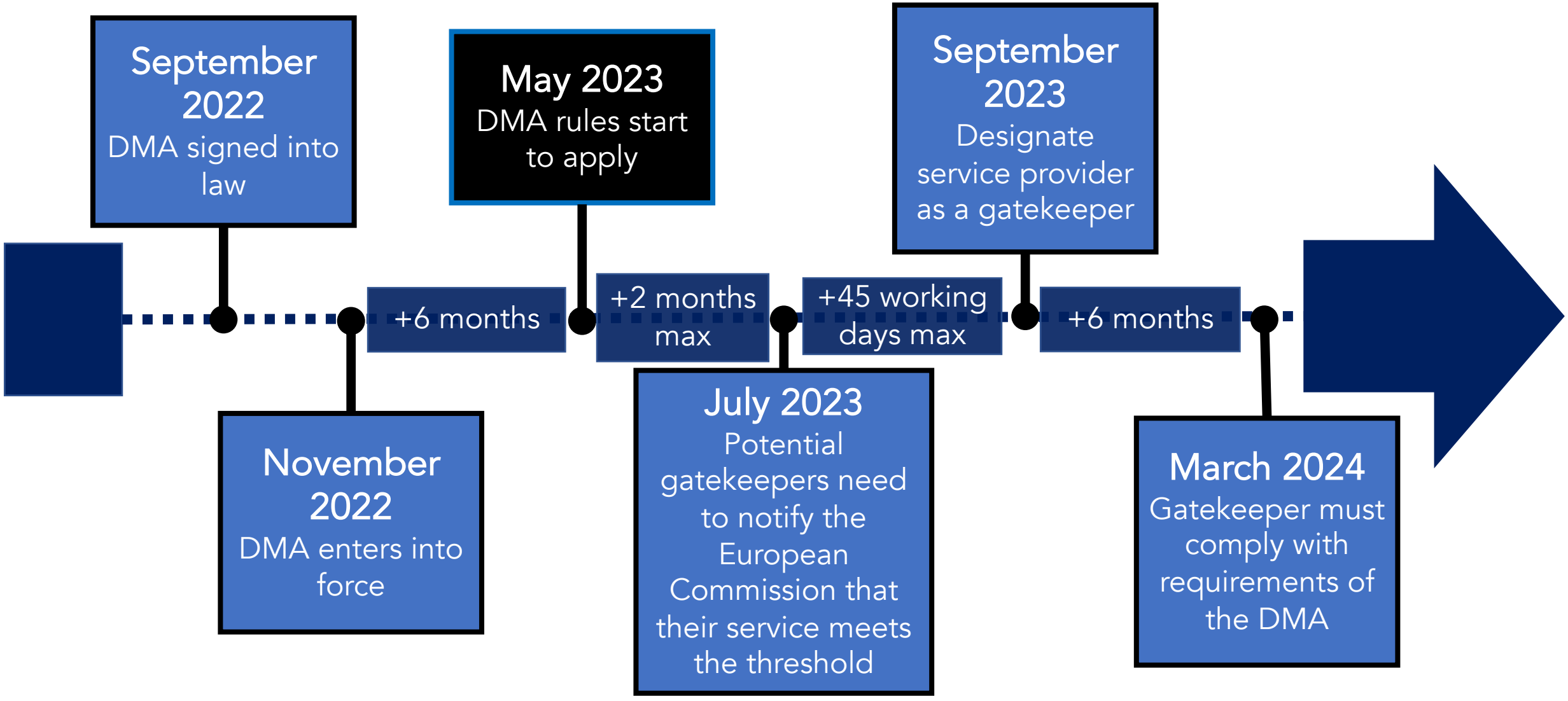
Open questions and opportunities of interoperability

# Digital Markets Act (DMA): Timeline



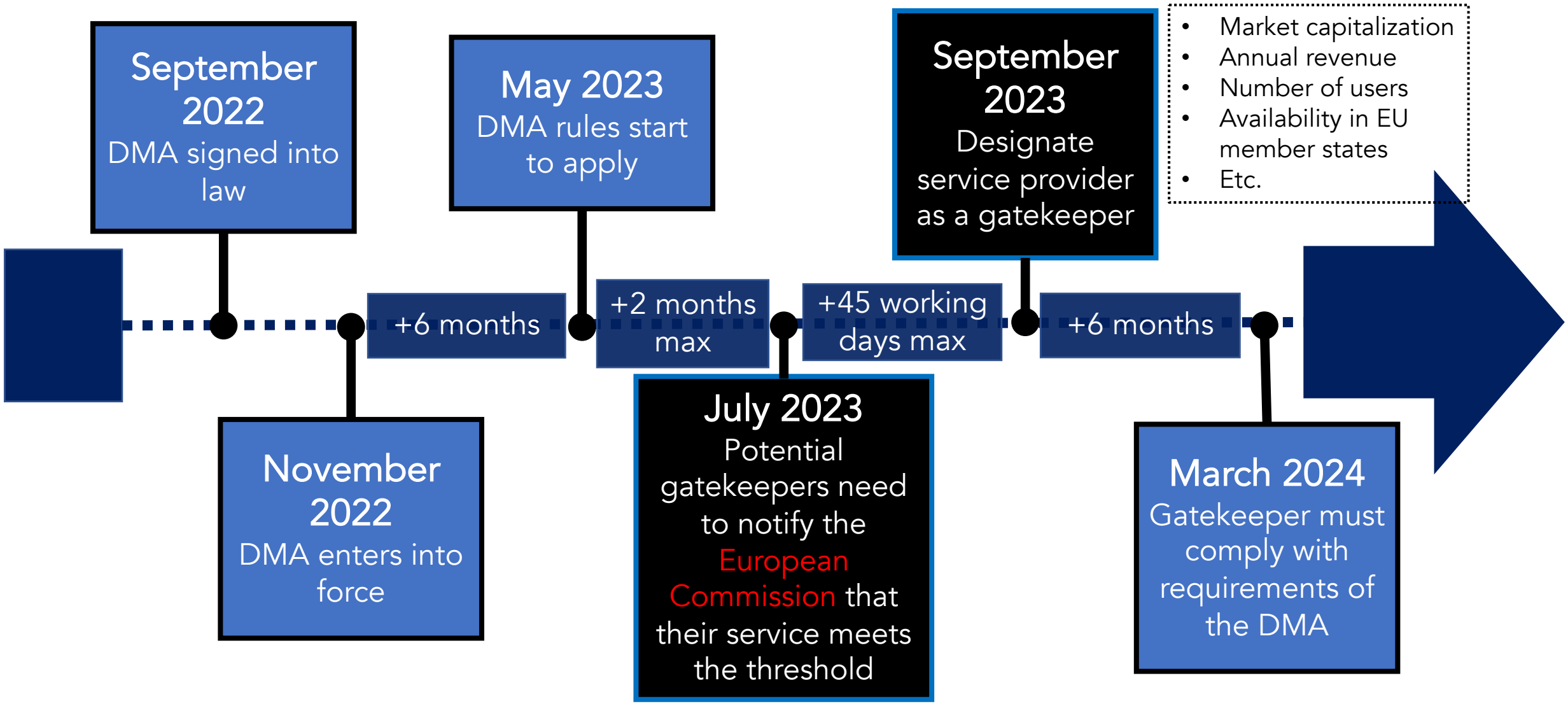

European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423

# Digital Markets Act (DMA): Timeline



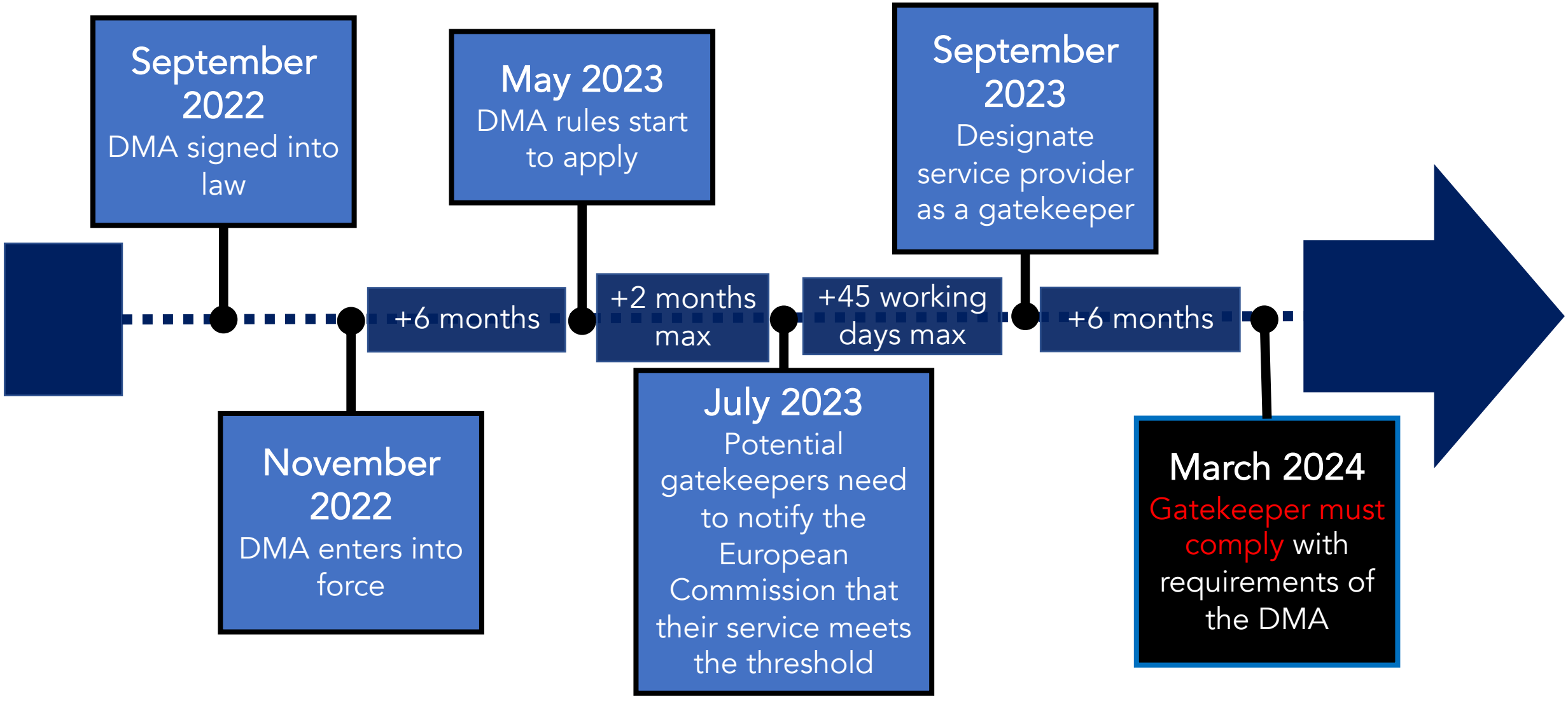

European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423

# Digital Markets Act (DMA): Timeline




European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423

# Digital Markets Act (DMA): Timeline




European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423

# DMA Article 7: Interoperability

So-called “gatekeepers” must provide the necessary technical interface (or equivalent) to enable interoperability with another provider upon request and free of charge

# DMA Article 7: Interoperability

So-called “gatekeepers” must provide the necessary technical interface (or equivalent) to enable interoperability with another provider upon request and free of charge

Requirements for basic functionalities (after designation as gatekeeper):

*After designation:*

Text messaging between two users

Sharing images, voice messages, videos, and other attached files between two users

# DMA Article 7: Interoperability

So-called “gatekeepers” must provide the necessary technical interface (or equivalent) to enable interoperability with another provider upon request and free of charge

Requirements for basic functionalities (after designation as gatekeeper):

*After designation:*

Text messaging between two users

Sharing images, voice messages, videos, and other attached files between two users

*2 years after designation:*

Extend functionality to group messaging

# DMA Article 7: Interoperability

So-called "gatekeepers" must provide the necessary technical interface (or equivalent) to enable interoperability with another provider upon request and free of charge

Requirements for basic functionalities (after designation as gatekeeper):

*After designation:*

Text messaging between two users

Sharing images, voice messages, videos, and other attached files between two users

*2 years after designation:*

Extend functionality to group messaging

*4 years after designation:*

Voice and video calls for both 1-1 and group communication

# DMA Article 7: Interoperability

## Paragraph 3 *(security)*

The level of security, including E2EE, that the gatekeeper provides to its own end users should be preserved for cross-platform messages

# DMA Article 7: Interoperability

## Paragraph 3 *(security)*

The level of security, including E2EE, that the gatekeeper provides to its own end users should be preserved for cross-platform messages

## Paragraph 8 *(privacy)*

Only the personal data of end users that is “strictly necessary” should be collected and exchanged by interoperating providers

# DMA Article 7: Interoperability

## Paragraph 3 *(security)*

The level of security, including E2EE, that the gatekeeper provides to its own end users should be preserved for cross-platform messages

## Paragraph 8 *(privacy)*

Only the personal data of end users that is “strictly necessary” should be collected and exchanged by interoperating providers

## Paragraph 9 *(abuse prevention)*

The gatekeeper is allowed to take measures to stop risk to “integrity, security, and privacy” of its services, as long as they are “strictly necessary”

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

Disclaimer: We are not lawyers or legal experts

Three components of messaging affected by the DMA:

1) Identity systems
2) E2EE protocols
3) Abuse prevention

Open questions and opportunities of interoperability

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

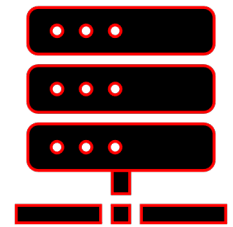
Disclaimer: We are not lawyers or legal experts

Three components of messaging affected by the DMA:

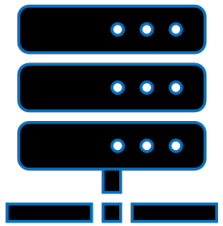
1) Identity systems
2) E2EE protocols
3) Abuse prevention

Open questions and opportunities of interoperability

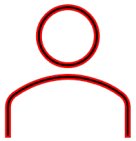
# Architecture



AliceChat



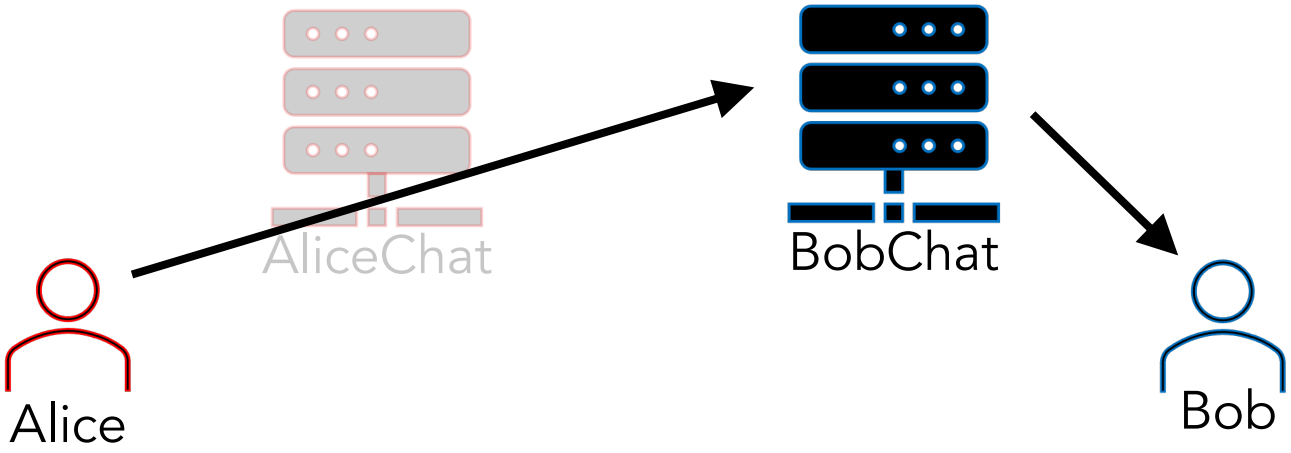
BobChat



Alice

Bob

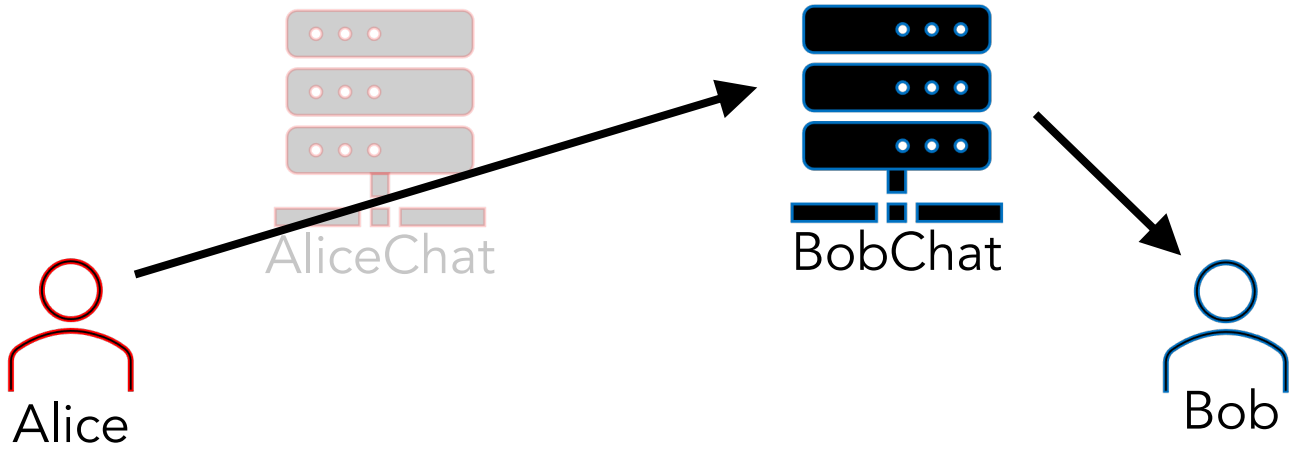
# Architecture




## Client-to-server

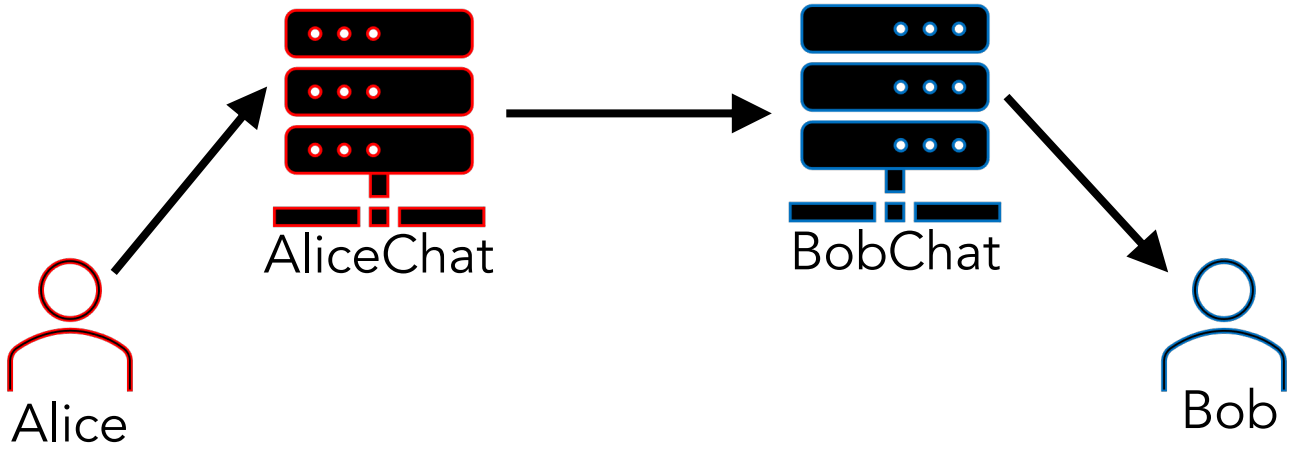
- \+ AliceChat does not learn that Alice is communicating with somebody on BobChat
- − Alice would need a way to authenticate herself to BobChat as an authorized user
- − Abuse prevention techniques like server-side spam filtering might be more challenging

# Architecture




## Client-to-server

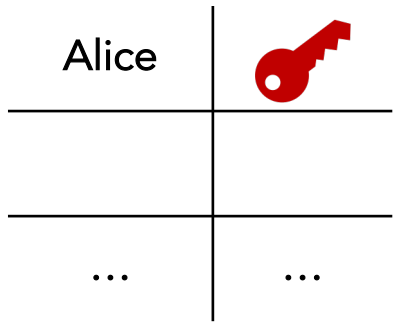
- ✚ AliceChat does not learn that Alice is communicating with somebody on BobChat
- — Alice would need a way to authenticate herself to BobChat as an authorized user
- — Abuse prevention techniques like server-side spam filtering might be more challenging

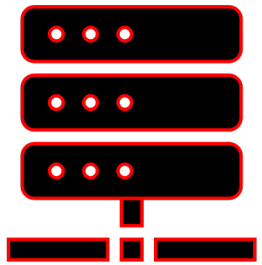


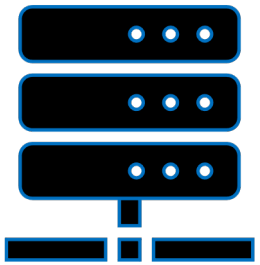

## Server-to-server (our design)

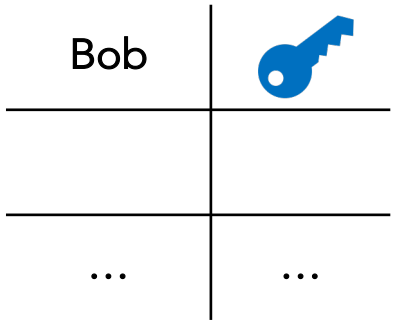
- — Leaks to AliceChat that Alice is talking to someone on BobChat and to BobChat that Bob is talking to someone on AliceChat
- ✚ Network-level metadata like IP addresses of users is not leaked in cross-provider communication to other providers
- ✚ Makes implementing some abuse prevention measures easier

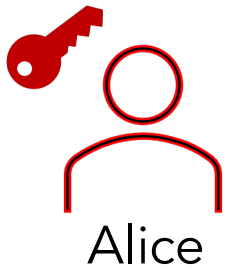
# Identity Discovery and Interoperability

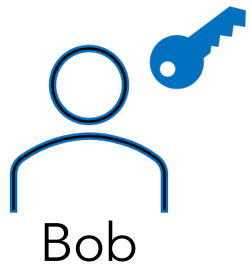


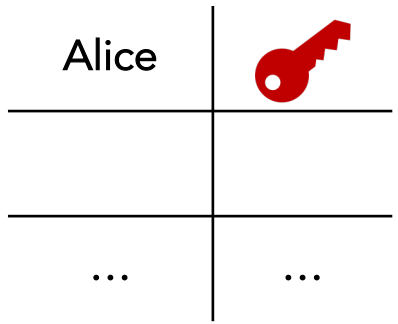



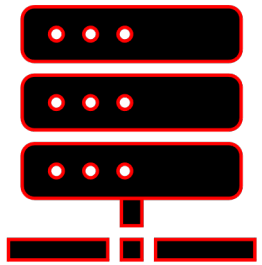



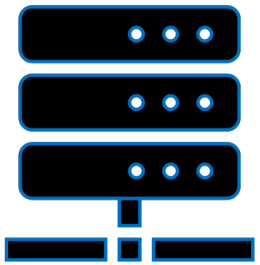



# Identity Discovery and Interoperability

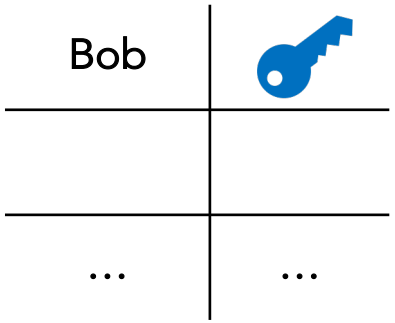


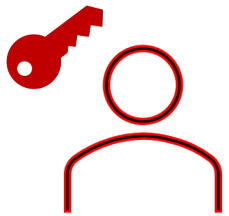



AliceChat



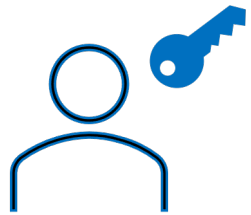
BobChat



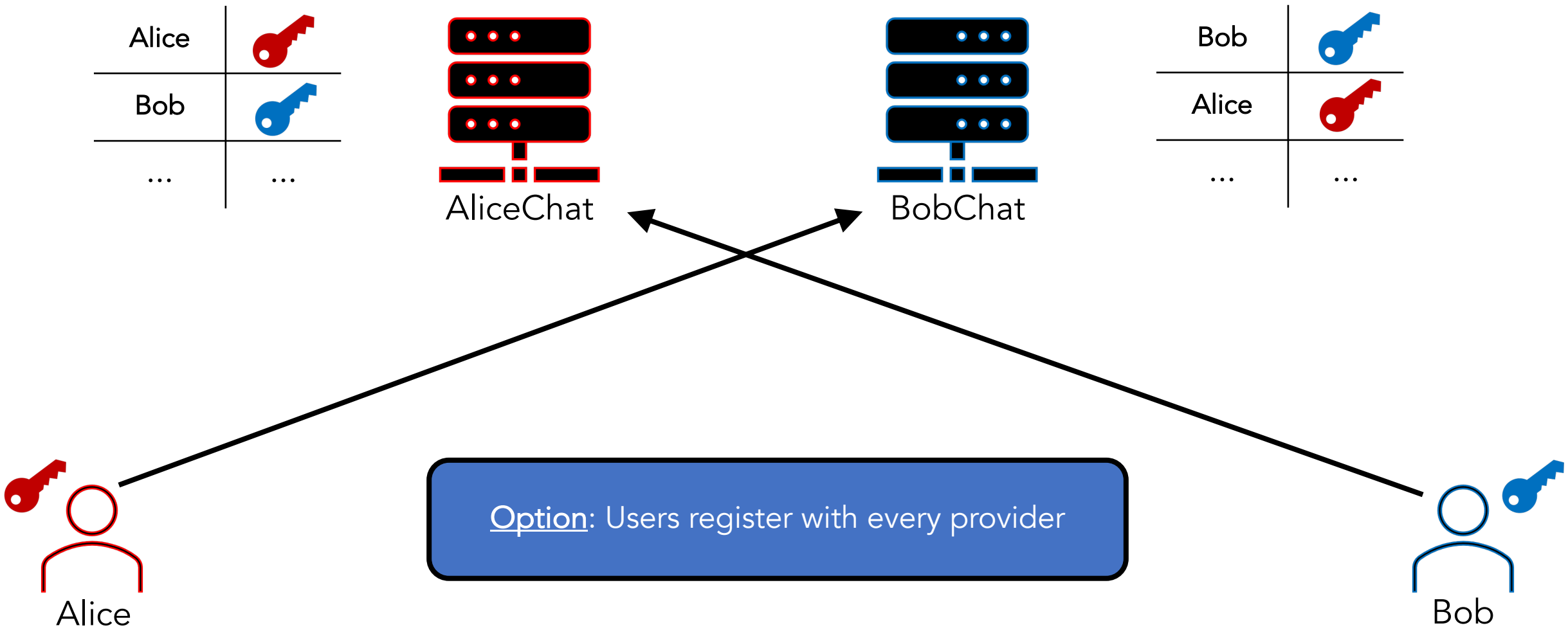
Alice

Option: Users register with every provider

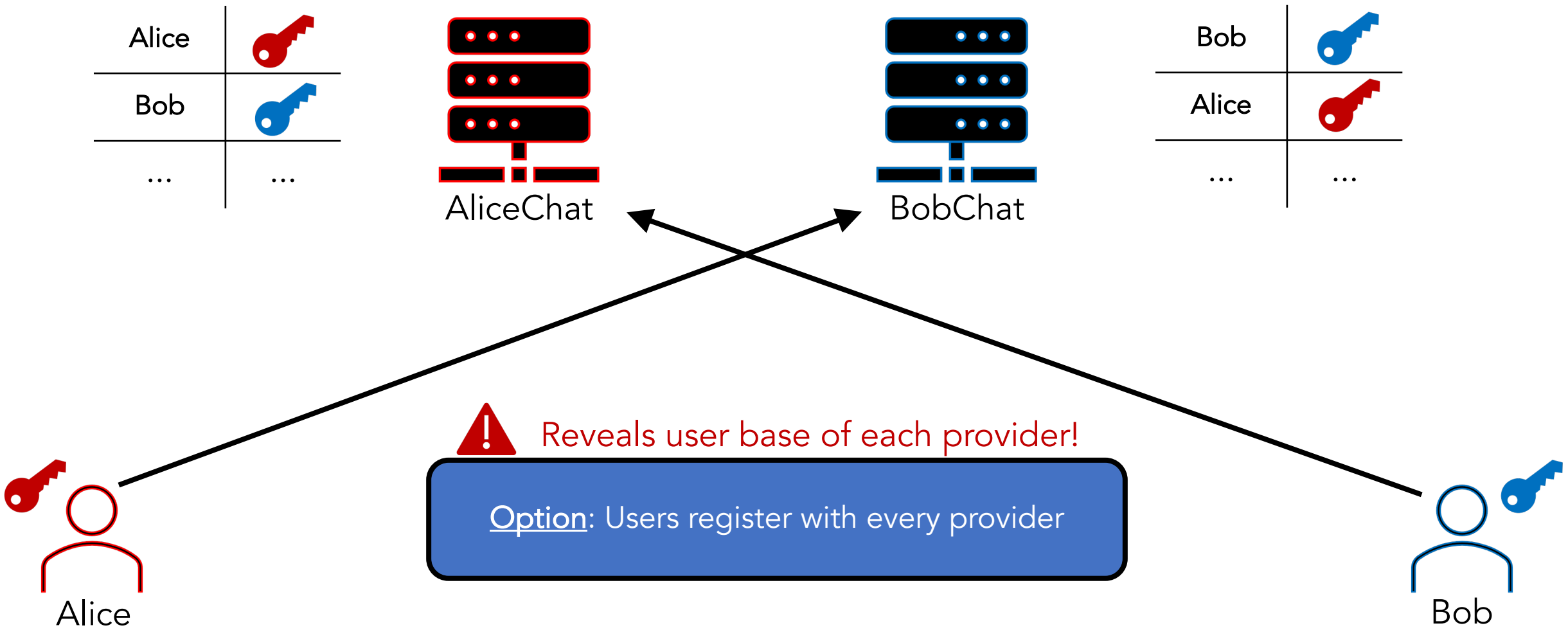


Bob

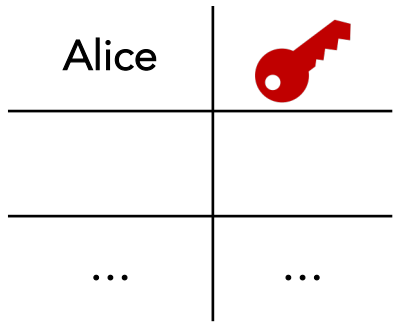
# Identity Discovery and Interoperability

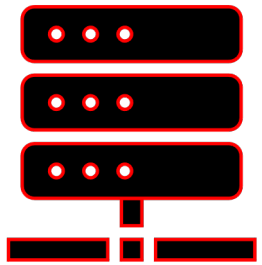


# Identity Discovery and Interoperability

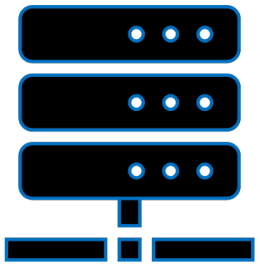


# Identity Discovery and Interoperability

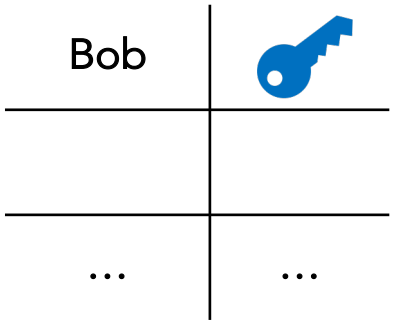


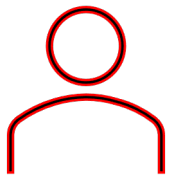



AliceChat



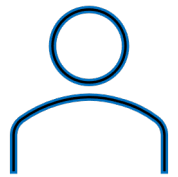
BobChat



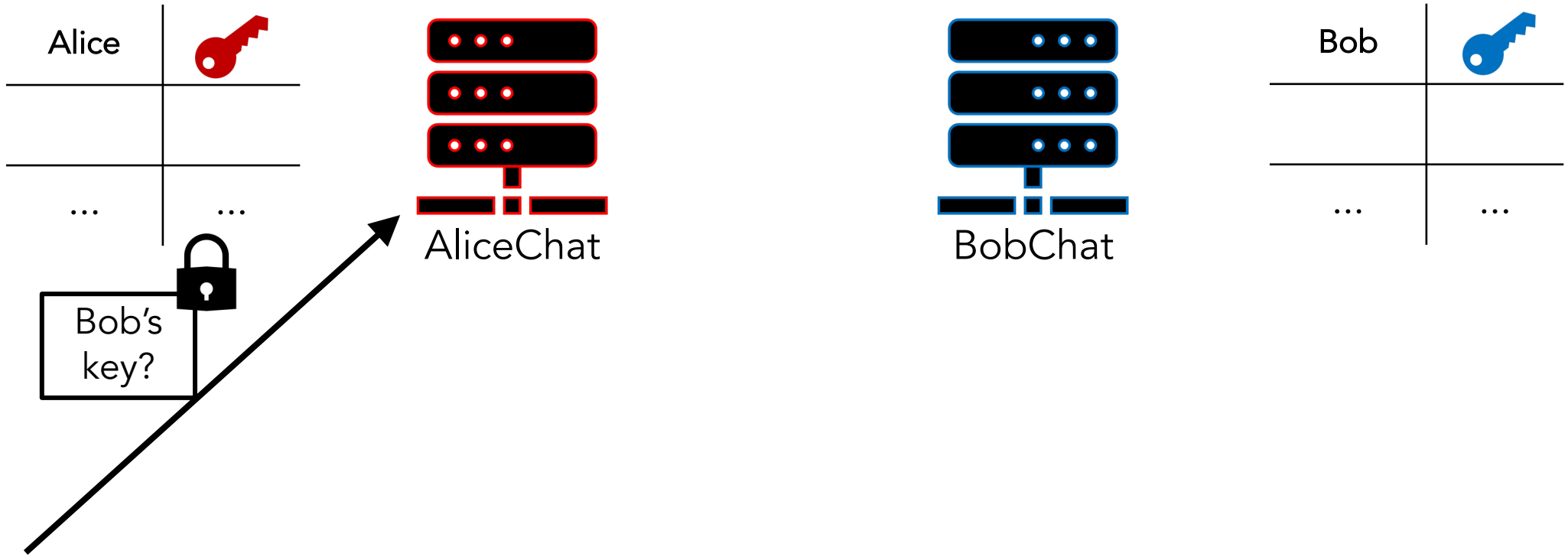
Alice

Our design: Encrypted queries to other provider's identity system

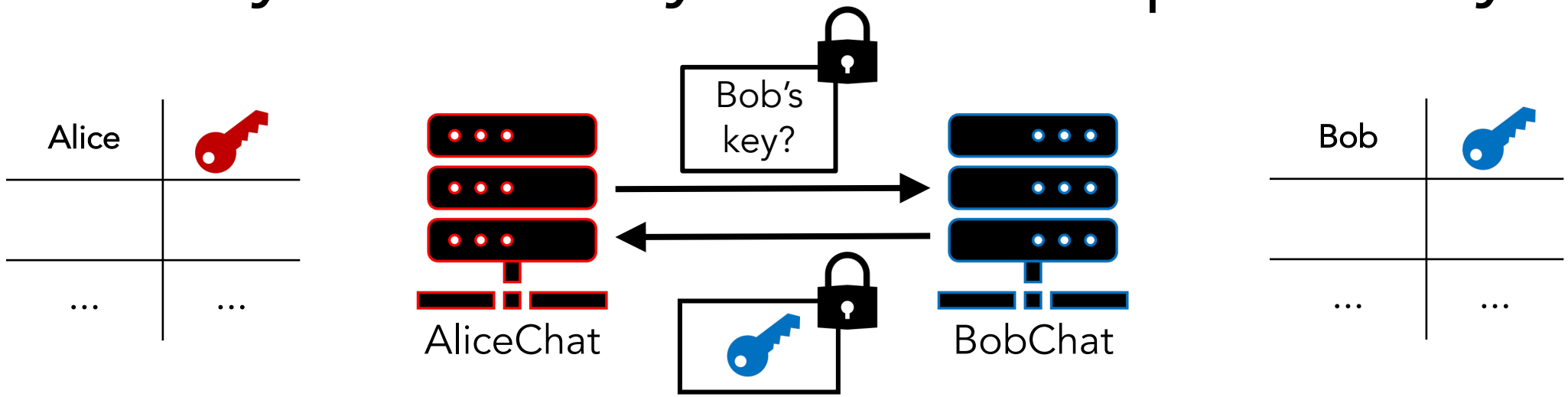


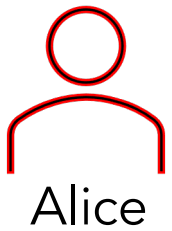
Bob

# Identity Discovery and Interoperability

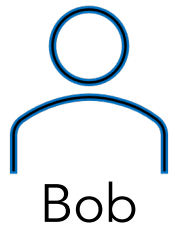


# Identity Discovery and Interoperability

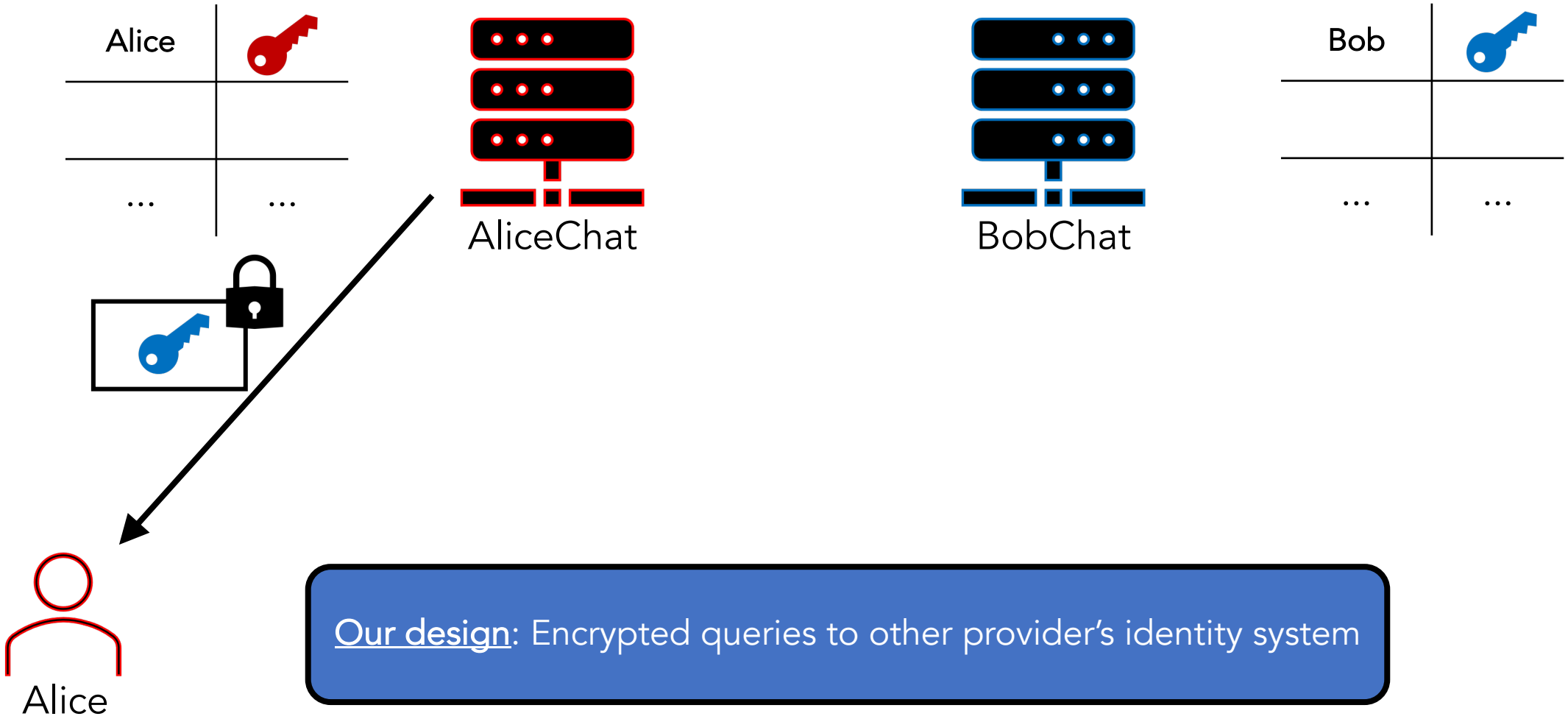


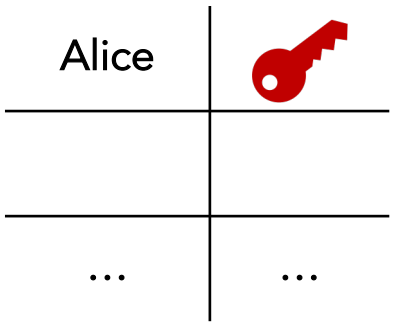

Our design: Encrypted queries to other provider's identity system

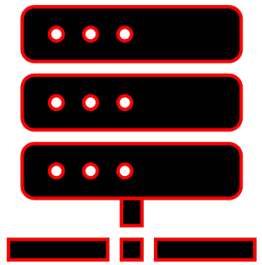


# Identity Discovery and Interoperability

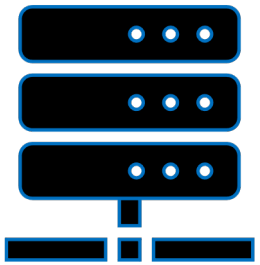


# Identity Discovery and Interoperability

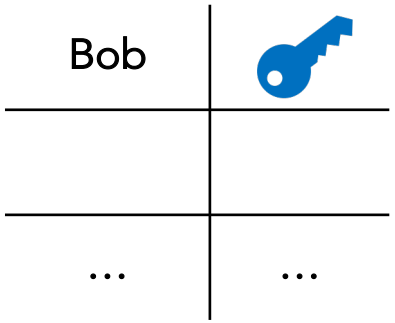


AliceChat

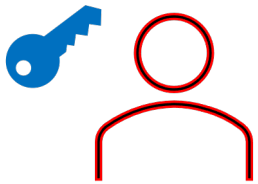


BobChat




**Security Goals**

- AliceChat should not learn Alice is querying for Bob
- BobChat should not learn Alice is the one querying

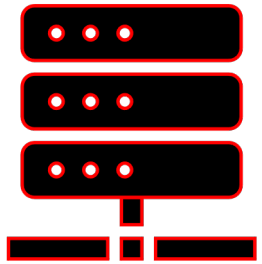


Alice

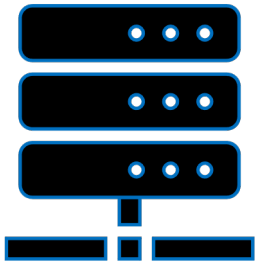
Our design: Encrypted queries to other provider's identity system

Bob

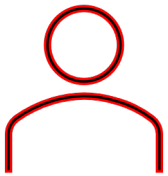
# Protocol-Layer Interoperability (PRO)



AliceChat



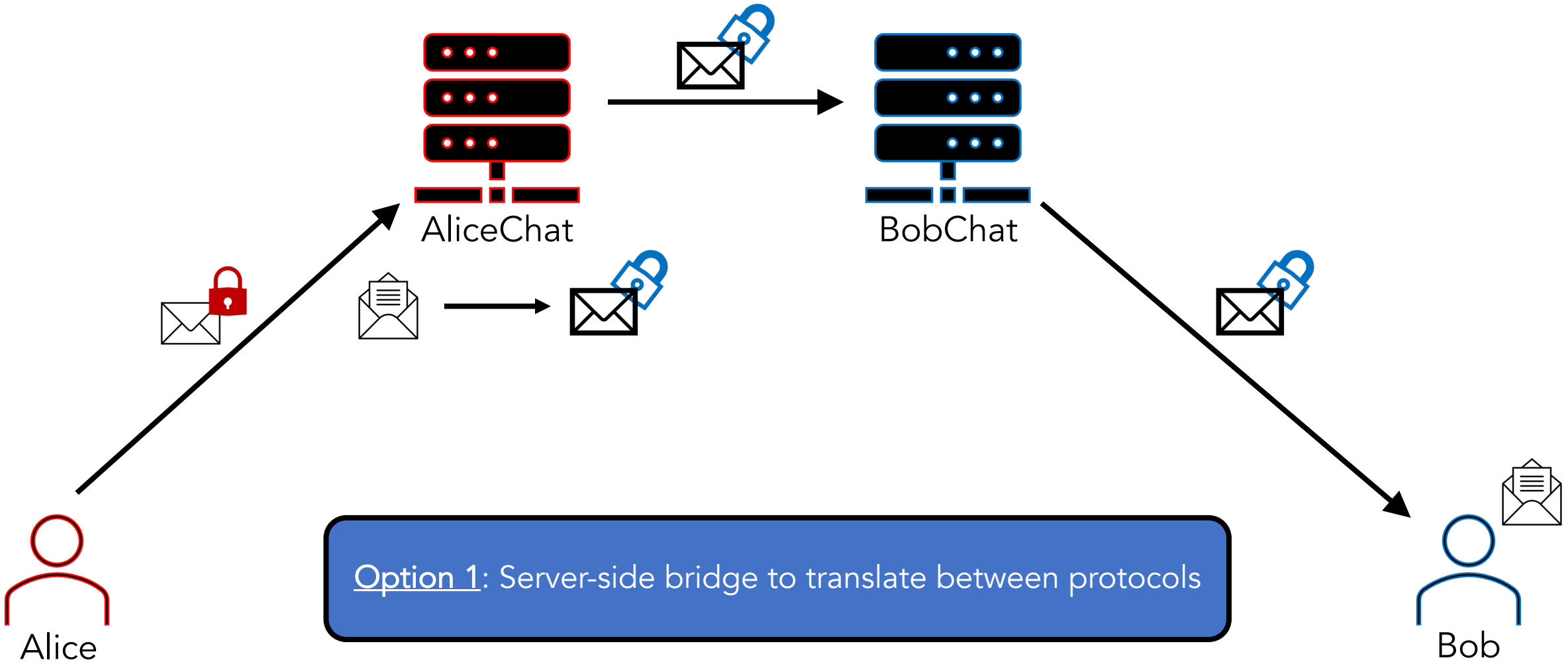
BobChat



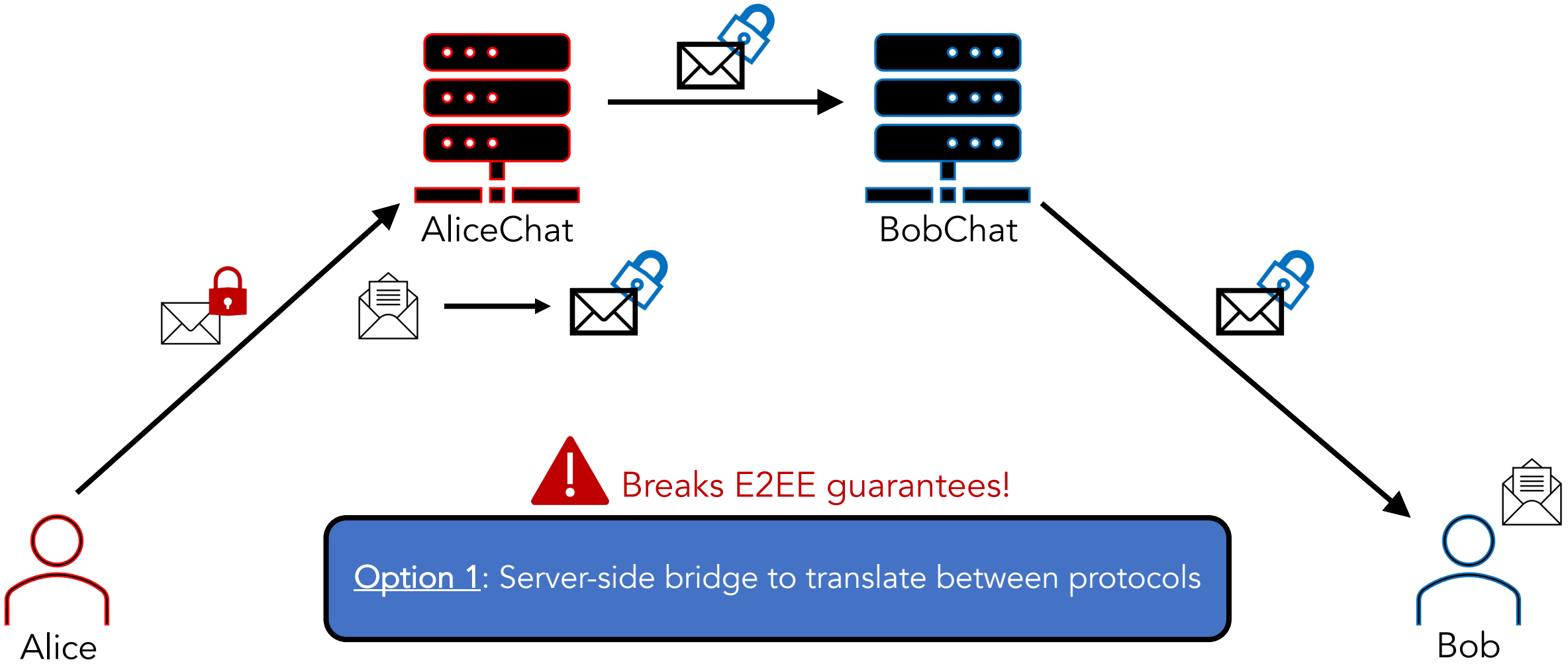
Alice

Bob

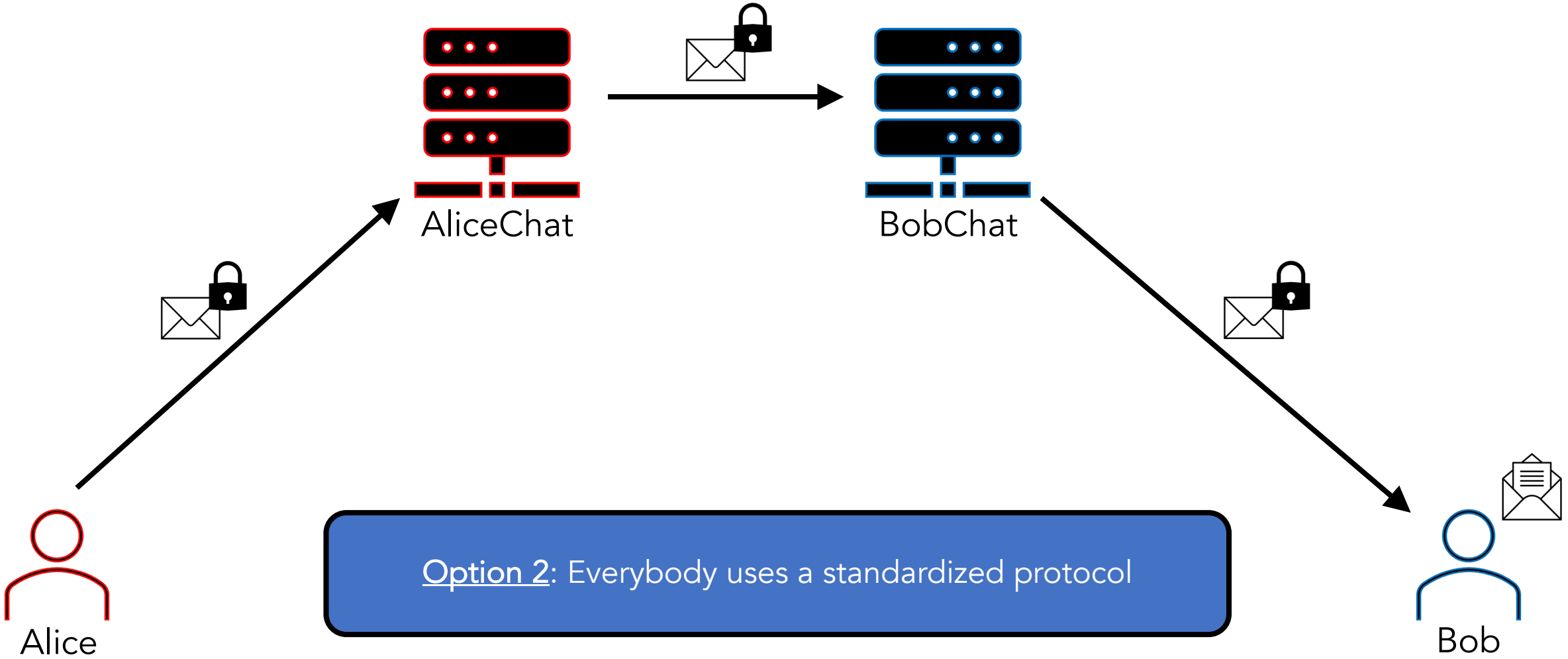
# Protocol-Layer Interoperability (PRO)



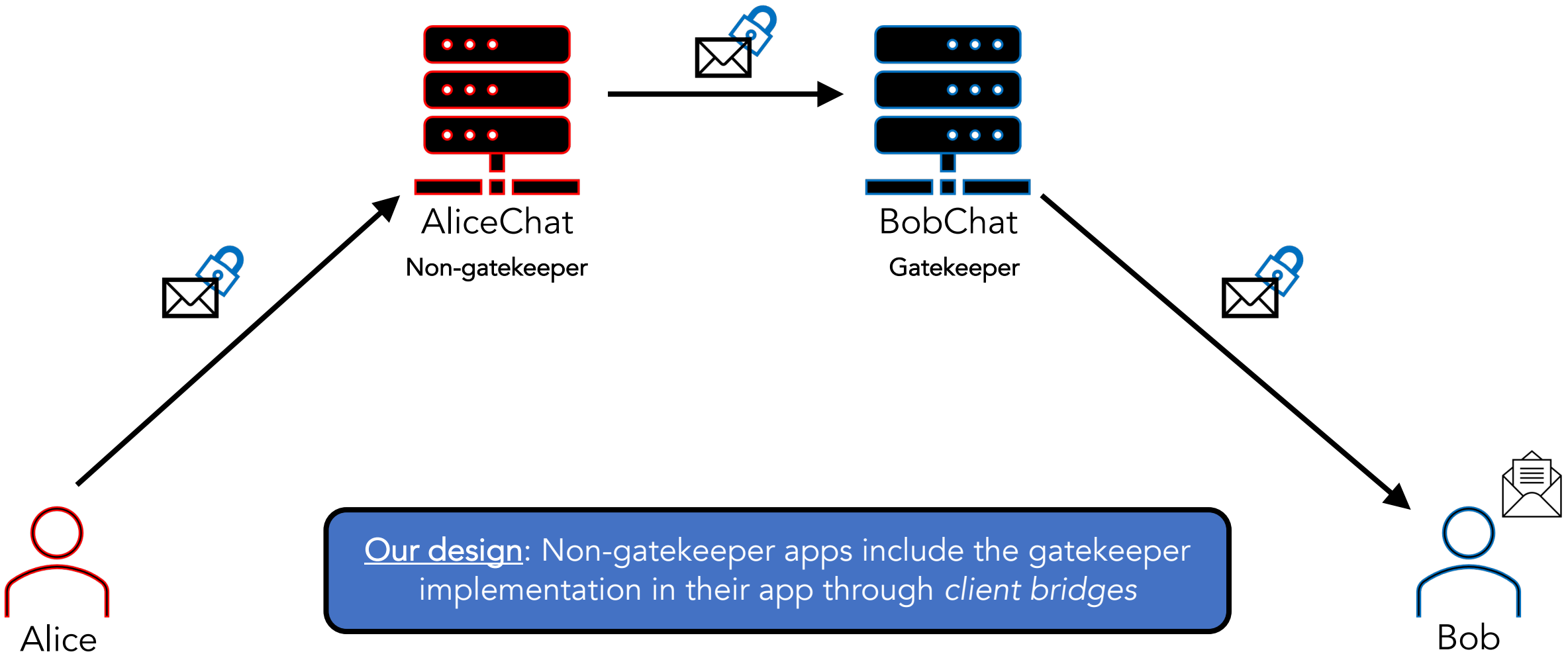
# Protocol-Layer Interoperability (PRO)



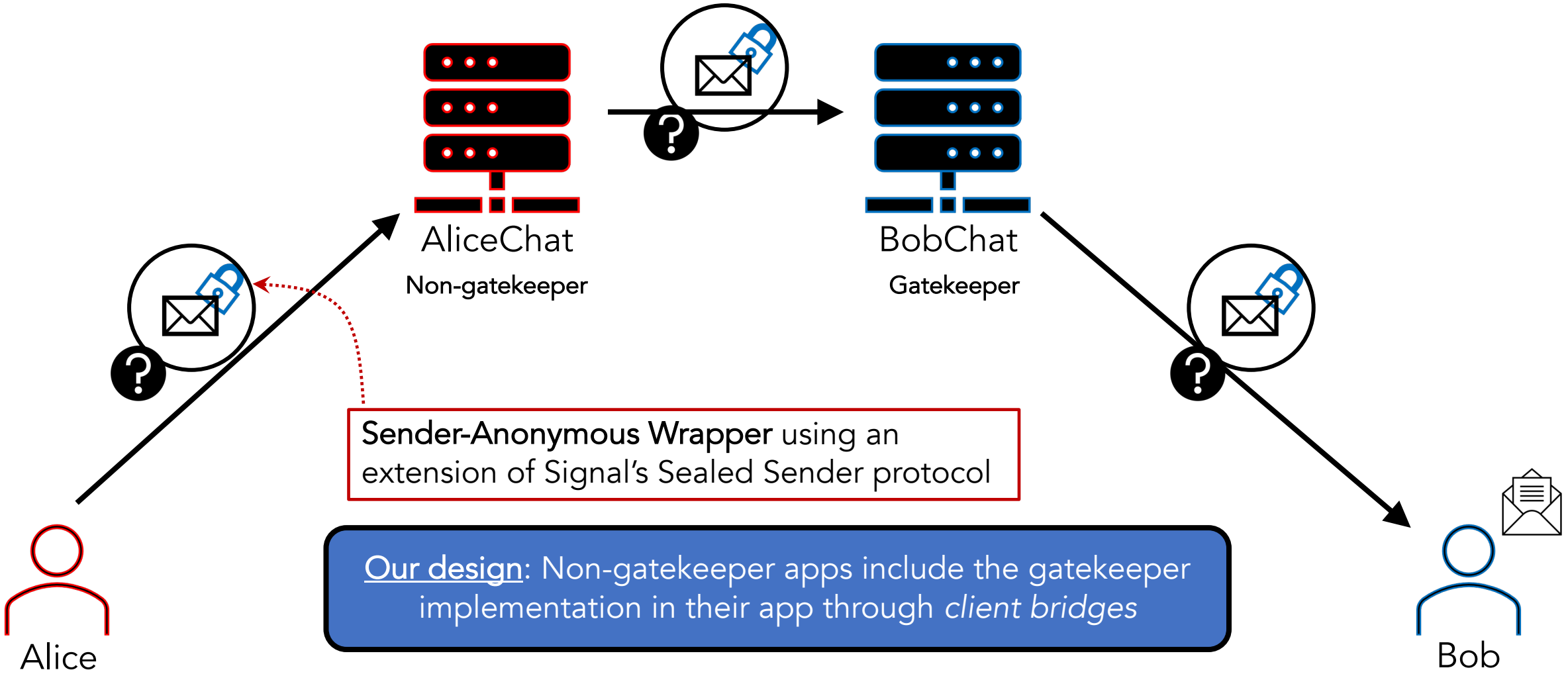
# Protocol-Layer Interoperability (PRO)



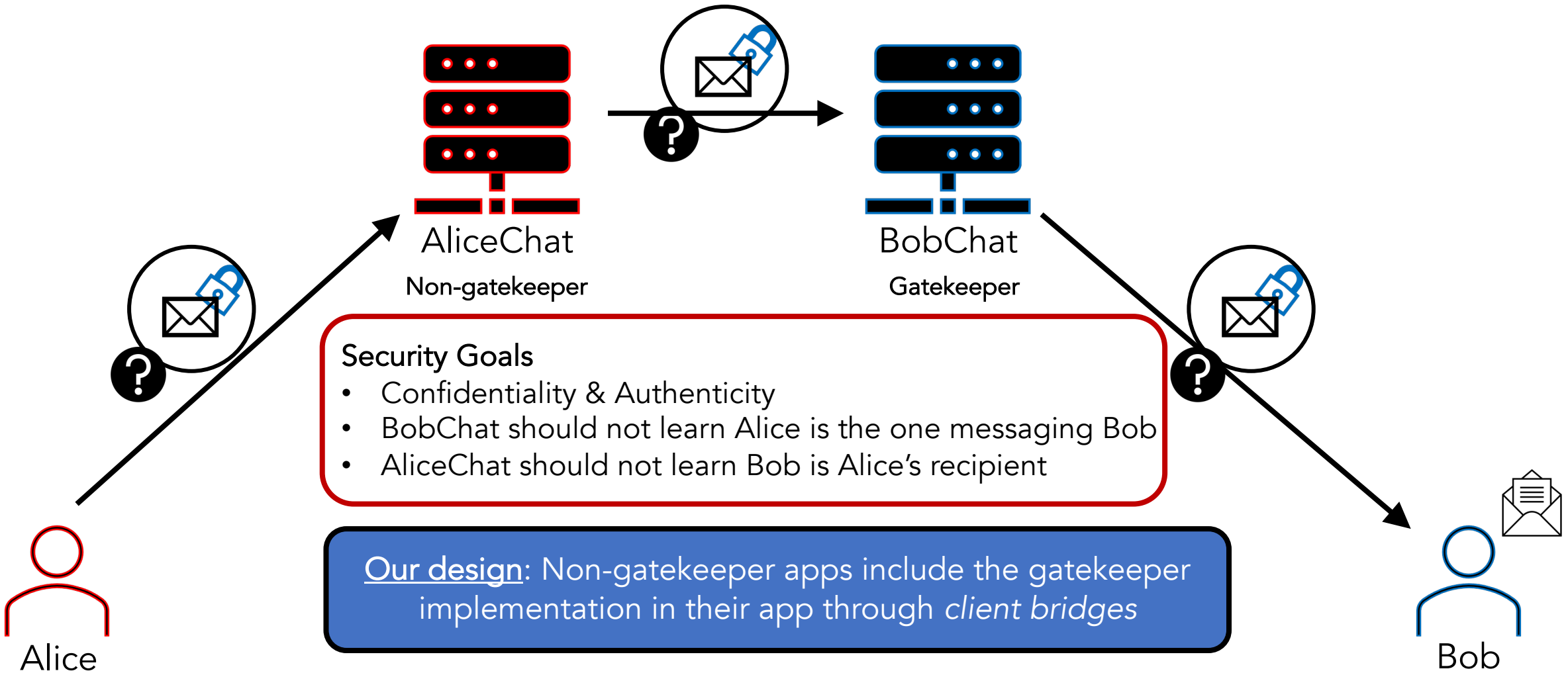
# Protocol-Layer Interoperability (PRO)



# Protocol-Layer Interoperability (PRO)



# Protocol-Layer Interoperability (PRO)

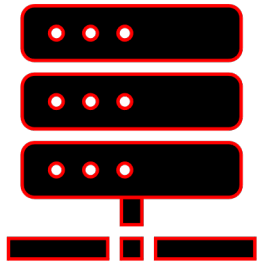



**Security Goals**

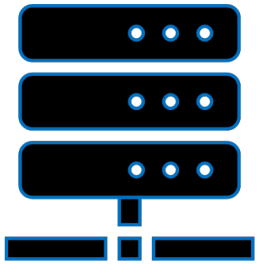
- Confidentiality & Authenticity
- BobChat should not learn Alice is the one messaging Bob
- AliceChat should not learn Bob is Alice's recipient

<u>Our design</u>: Non-gatekeeper apps include the gatekeeper implementation in their app through *client bridges*

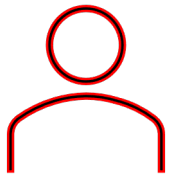
# Abuse Prevention (ABP)



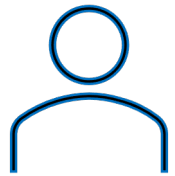
AliceChat



BobChat

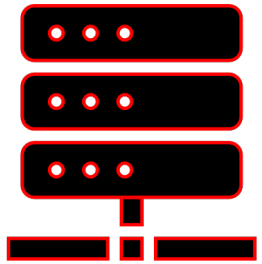


Alice

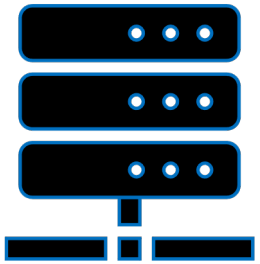


Bob

# Abuse Prevention (ABP)

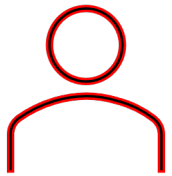


AliceChat



BobChat

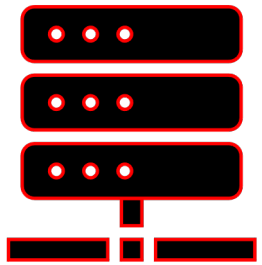
<u>Option 1</u>: Don’t address it



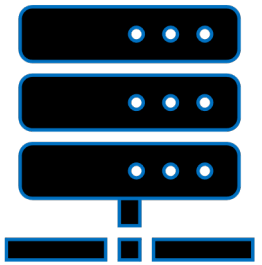
Alice

Bob

# Abuse Prevention (ABP)



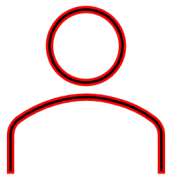
AliceChat



BobChat

Bad for privacy!

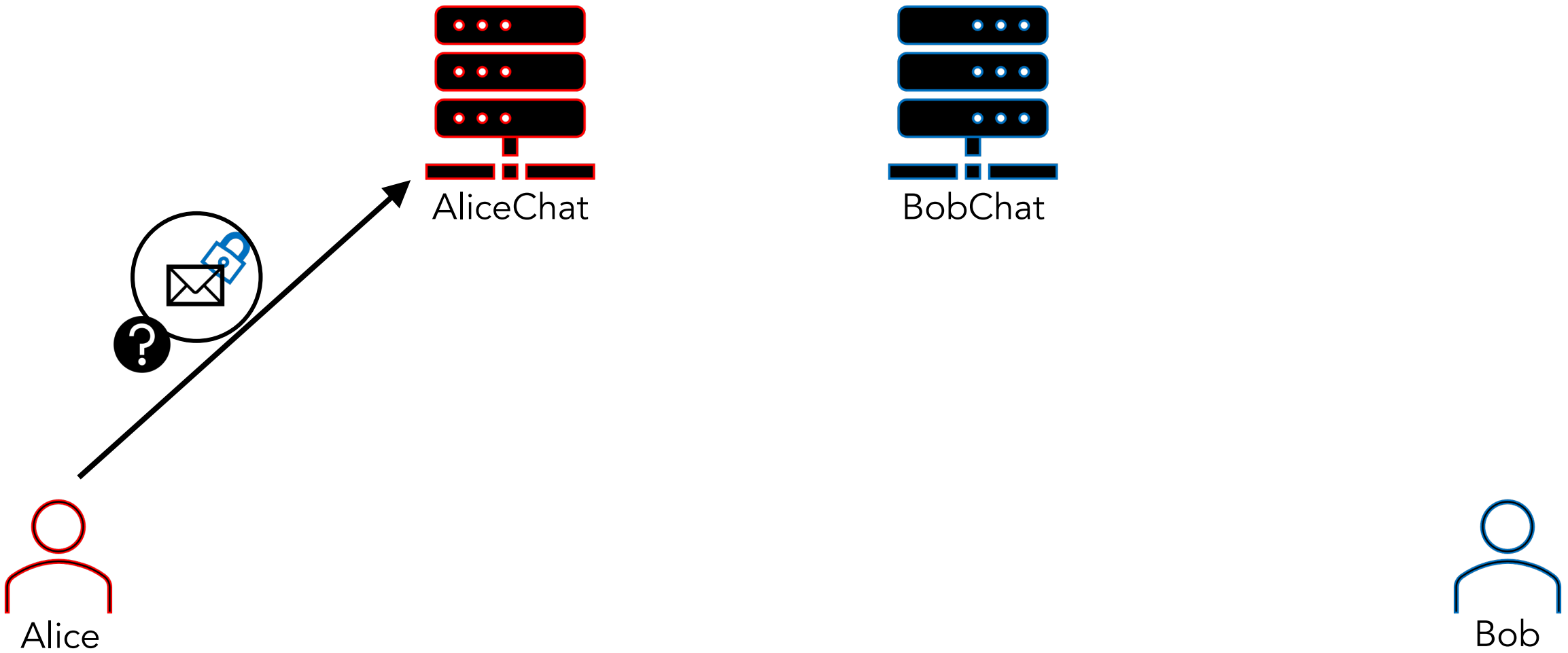
<u>Option 2</u>: Give BobChat all the metadata about senders from AliceChat.



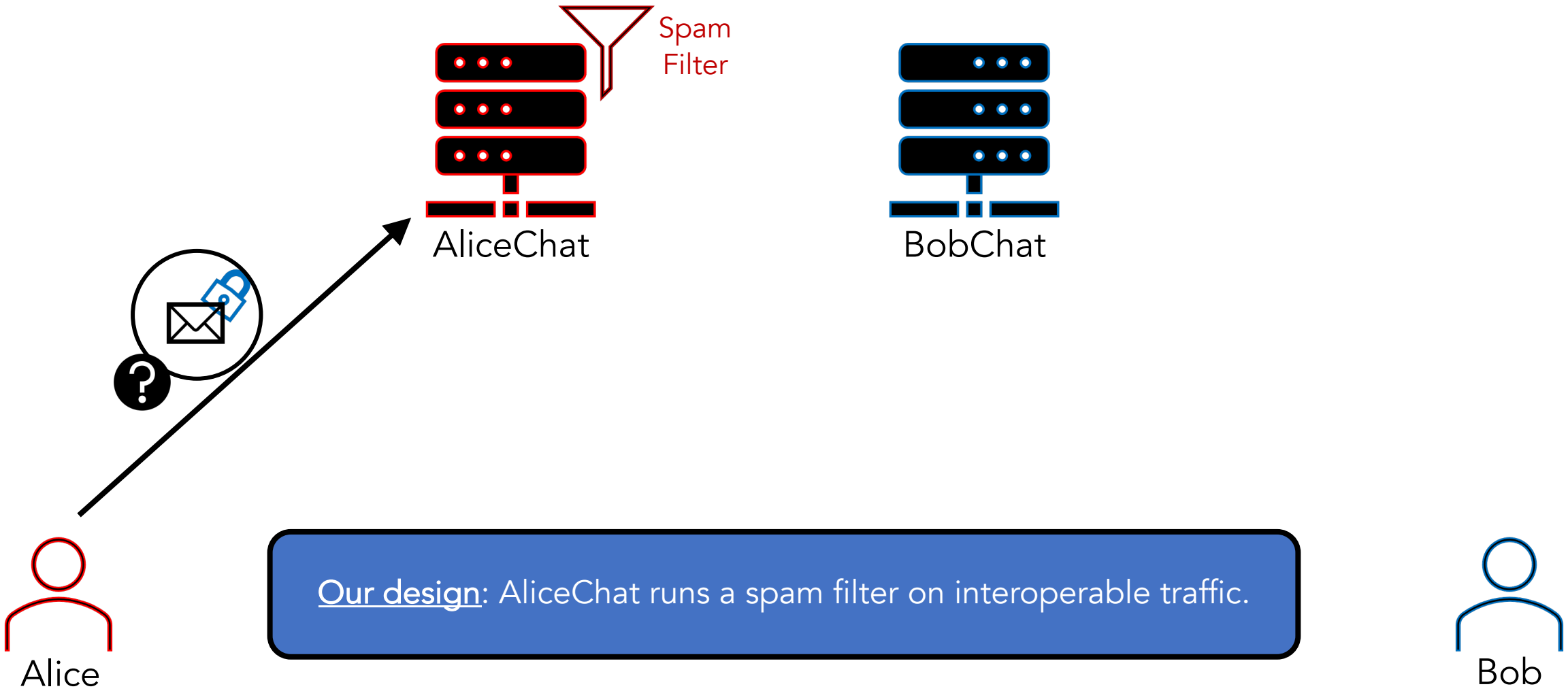
Alice

Bob

# Abuse Prevention (ABP): Spam Filtering

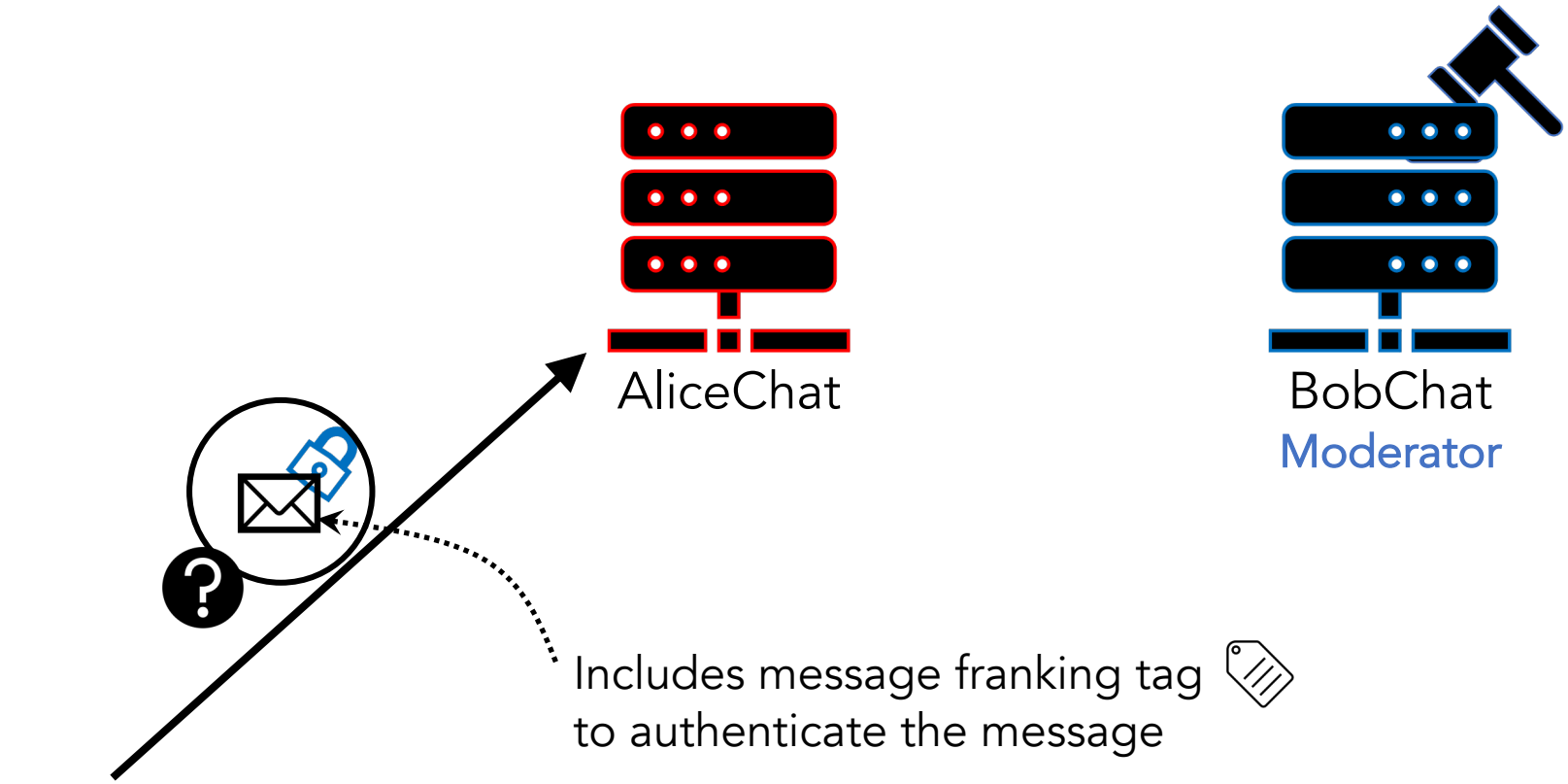


# Abuse Prevention (ABP): Spam Filtering




Our design: AliceChat runs a spam filter on interoperable traffic.

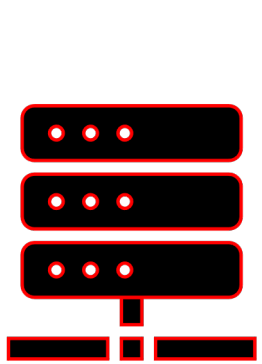
# Abuse Prevention (ABP): User Reporting



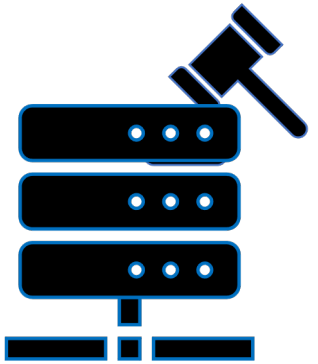

Our design: Use an *Asymmetric Message Franking* [TGLMR19] scheme to enable secure metadata-private moderation.

Nirvan Tyagi, Paul Grubbs, Julia Len, Ian Miers, and Thomas Ristenpart. Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption. CRYPTO 2019.

# Abuse Prevention (ABP): User Reporting

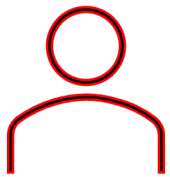


AliceChat



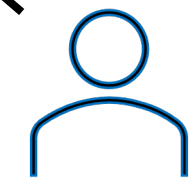
BobChat
Moderator


Sent by Alice



Alice

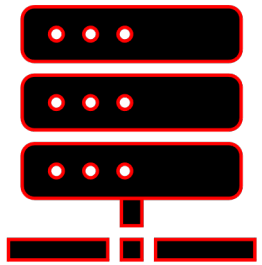
**Our design**: Use an *Asymmetric Message Franking* [TGLMR19] scheme to enable secure metadata-private moderation.



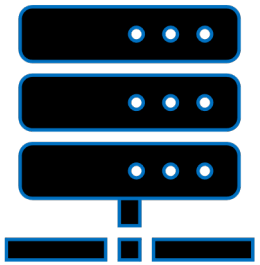
Bob

Nirvan Tyagi, Paul Grubbs, Julia Len, Ian Miers, and Thomas Ristenpart. Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption. CRYPTO 2019.

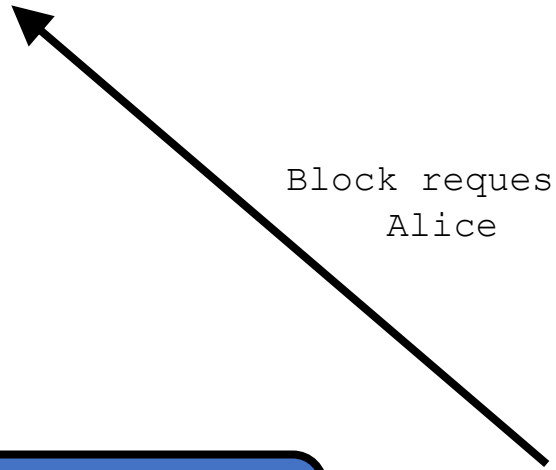
# Abuse Prevention (ABP): Blocklisting

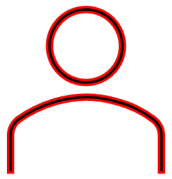


AliceChat



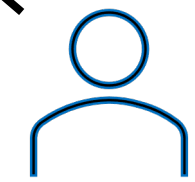
BobChat



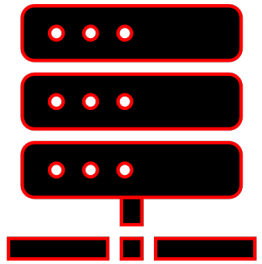
Alice

<u>Our design</u>: Bob reveals Alice's user id to BobChat and BobChat knows the identity of those wanting to initiate communication.

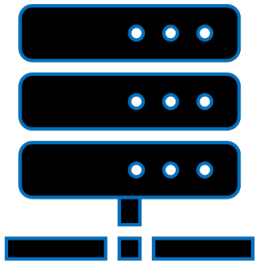


Bob

# Abuse Prevention (ABP)



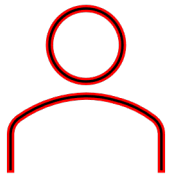
AliceChat



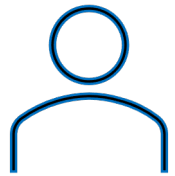
BobChat

**Security Goals**

- Verifiable user reporting
- Minimize metadata leakage



Alice



Bob

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

Disclaimer: We are not lawyers or legal experts

Three components of messaging affected by the DMA:

1) Identity systems
2) E2EE protocols
3) Abuse prevention

Open questions and opportunities of interoperability

# Our Goals

*Given the DMA and its timeline, how can the existing components of widely used E2EE apps be extended to be interoperable?*

Overview of the Digital Markets Act (DMA) interoperability requirements

Disclaimer: We are not lawyers or legal experts

Three components of messaging affected by the DMA:

1) Identity systems
2) E2EE protocols
3) Abuse prevention

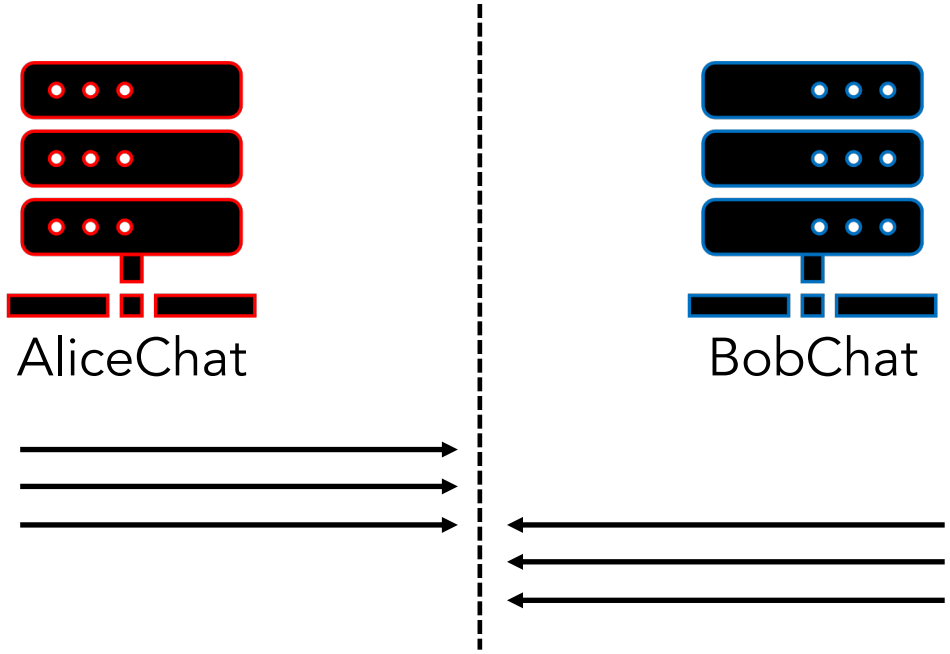
Open questions and opportunities of interoperability

# Open Problems in Interoperable E2EE

- How do we improve the privacy of interoperable E2EE by reducing metadata leakage?
- How do we extend other protocols used in E2EE messaging, like key transparency, into the interoperability setting?
- How do we extend our framework and analyses to group chats and encrypted calls?

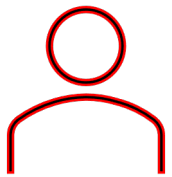
# Conclusion: This is an Opportunity

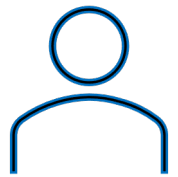
https://ia.cr/2023/386




**Free privacy win from our server-to-server architecture!**

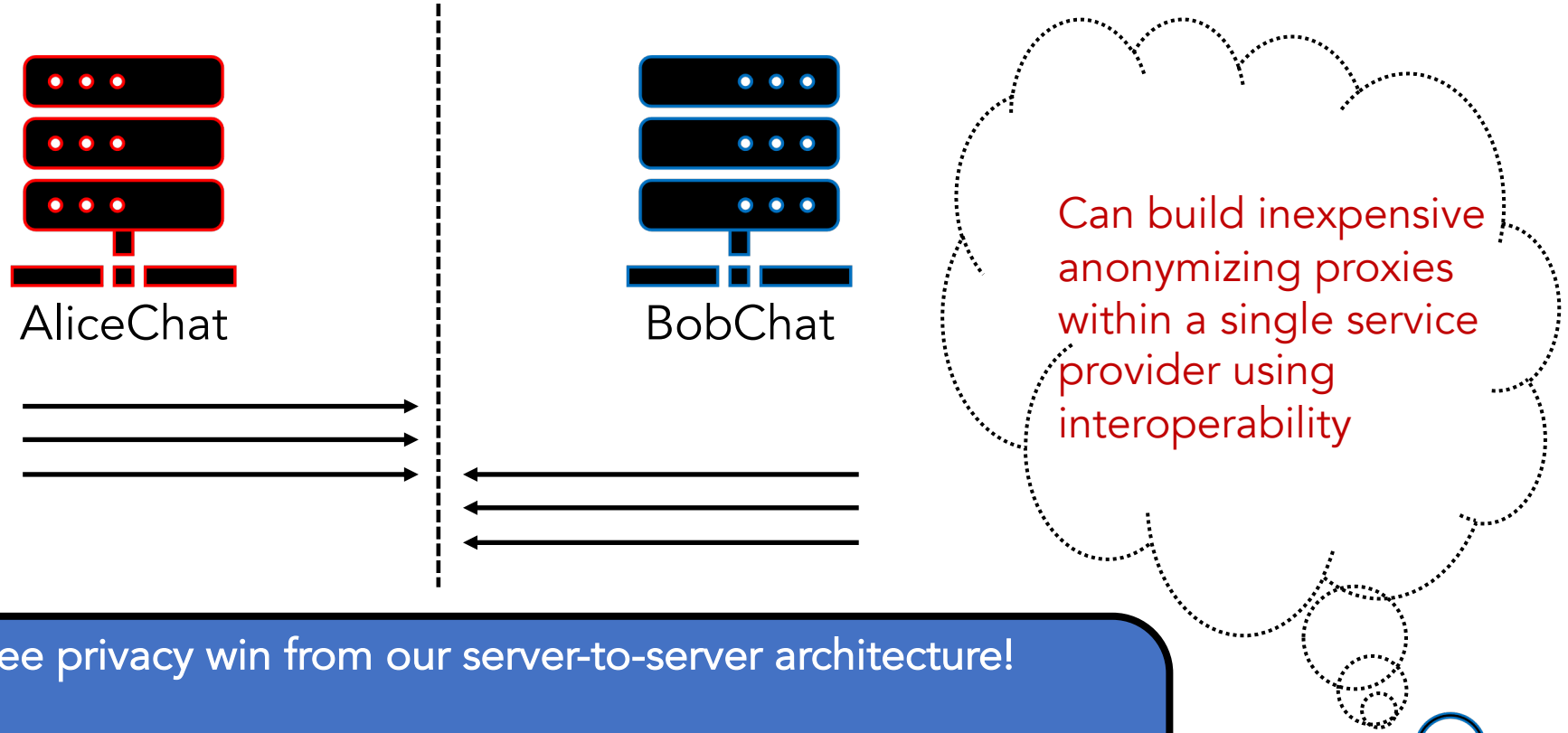
- We can hide network-level metadata from the other provider in cross-provider traffic
- Better privacy than in Signal's Sealed Sender (which does not hide network-level metadata)



# Conclusion: This is an Opportunity

https://ia.cr/2023/386




**Free privacy win from our server-to-server architecture!**

- We can hide network-level metadata from the other provider in cross-provider traffic
- Better privacy than in Signal's Sealed Sender (which does not hide network-level metadata)