Interoperability in E2EE Messaging

Julia Len
Cornell Tech
jlen@cs.cornell.edu

Esha Ghosh
Microsoft Research
esha.ghosh@microsoft.com

Paul Grubbs
University of Michigan
paulgrub@umich.edu

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

WhatsApp

Signal
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
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

WhatsApp

Signal
End-to-End Encrypted Messaging Today

Interoperability request
End-to-End Encrypted Messaging Today
End-to-End Encrypted Messaging Today

WhatsApp

Deadline: March 2024

Signal
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

Service Provider 2

Charlie
charlie@email.com

Dan
dan@email.com

Phone numbers as user identifiers

Email as user identifiers
New Challenges

Alice
(111)111-1111

Service Provider 1

Bob
(222)222-2222

Charlie
charlie@email.com

Uses Signal’s Double Ratchet algorithm for E2EE protocol

Uses MTProto algorithm for E2EE protocol

Dan
dan@email.com

Service Provider 2
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.

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>Service Provider 1</th>
<th>Abuse report</th>
</tr>
</thead>
<tbody>
<tr>
<td>(111)111-1111</td>
<td>(222)222-2222</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td>Dan</td>
<td>Service Provider 2</td>
<td>Abuse report</td>
</tr>
<tr>
<td>#@$%!</td>
<td>#@$%!</td>
<td><a href="mailto:charlie@email.com">charlie@email.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:dan@email.com">dan@email.com</a></td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>BLOCKED</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

Service Provider 1

Alice
(111)111-1111

Bob
(222)222-2222

Charlie
charlie@email.com

Service Provider 2

Dan
dan@email.com
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

- **September 2022**: DMA signed into law
- **November 2022**: DMA enters into force
- **May 2023**: DMA rules start to apply
- **September 2023**: Designate service provider as a gatekeeper
- **July 2023**: Potential gatekeepers need to notify the European Commission that their service meets the threshold
- **March 2024**: Gatekeeper must comply with requirements of the DMA

Digital Markets Act (DMA): Timeline

- **September 2022**: DMA signed into law
- **November 2022**: DMA enters into force
- **May 2023**: DMA rules start to apply
  - +6 months
  - +2 months max
  - +45 working days max
- **September 2023**: Designate service provider as a gatekeeper
  - +6 months
- **July 2023**: Potential gatekeepers need to notify the European Commission that their service meets the threshold
- **March 2024**: Gatekeeper must comply with requirements of the DMA
  - +6 months

Digital Markets Act (DMA): Timeline

- **September 2022**: DMA signed into law
- **November 2022**: DMA enters into force
- **May 2023**: DMA rules start to apply
- **September 2023**: Designate service provider as a gatekeeper
- **July 2023**: Potential gatekeepers need to notify the European Commission that their service meets the threshold
- **March 2024**: Gatekeeper must comply with requirements of the DMA

- Market capitalization
- Annual revenue
- Number of users
- Availability in EU member states
- Etc.

Digital Markets Act (DMA): Timeline

- **September 2022**: DMA signed into law
- **November 2022**: DMA enters into force
- **May 2023**: DMA rules start to apply
- **September 2023**: Designate service provider as a gatekeeper
- **July 2023**: Potential gatekeepers need to notify the European Commission that their service meets the threshold
- **March 2024**: Gatekeeper must comply with requirements of the DMA

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):

- 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
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.
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
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.

AliceChat does not learn that Alice is communicating with somebody on BobChat.
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

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

AliceChat

BobChat

Alice

Bob
Identity Discovery and Interoperability

Option: Users register with every provider
Identity Discovery and Interoperability

Option: Users register with every provider
Identity Discovery and Interoperability

Option: Users register with every provider

Reveals user base of each provider!
Identity Discovery and Interoperability

**Our design:** Encrypted queries to other provider’s identity system
Identity Discovery and Interoperability

Our design: Encrypted queries to other provider's identity system
Identity Discovery and Interoperability

Our design: Encrypted queries to other provider’s identity system
Identity Discovery and Interoperability

**Our design:** Encrypted queries to other provider’s identity system
Identity Discovery and Interoperability

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

Our design: Encrypted queries to other provider's identity system
Protocol-Layer Interoperability (PRO)
Protocol-Layer Interoperability (PRO)

Option 1: Server-side bridge to translate between protocols
Protocol-Layer Interoperability (PRO)

Option 1: Server-side bridge to translate between protocols

Breaks E2EE guarantees!
Protocol-Layer Interoperability (PRO)

Option 2: Everybody uses a standardized protocol
Protocol-Layer Interoperability (PRO)

Our design: Non-gatekeeper apps include the gatekeeper implementation in their app through client bridges
Our design: Non-gatekeeper apps include the gatekeeper implementation in their app through *client bridges*. 

**Sender-Anonymous Wrapper** using an extension of Signal’s Sealed Sender protocol
Protocol-Layer Interoperability (PRO)

Our design: Non-gatekeeper apps include the gatekeeper implementation in their app through client bridges

Security Goals
- Confidentiality & Authenticity
- BobChat should not learn Alice is the one messaging Bob
- AliceChat should not learn Bob is Alice’s recipient
Abuse Prevention (ABP)
Abuse Prevention (ABP)

Option 1: Don’t address it
Abuse Prevention (ABP)

Option 2: Give BobChat all the metadata about senders from AliceChat.

Bad for privacy!
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.
Abuse Prevention (ABP): User Reporting

Our design: Use an Asymmetric Message Franking [TGLMR19] scheme to enable secure metadata-private moderation.
Abuse Prevention (ABP): Blocklisting

Our design: Bob reveals Alice’s user id to BobChat and BobChat knows the identity of those wanting to initiate communication.
Abuse Prevention (ABP)

Security Goals

• Verifiable user reporting
• Minimize metadata leakage
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

Can build inexpensive anonymizing proxies within a single service provider using interoperability

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)