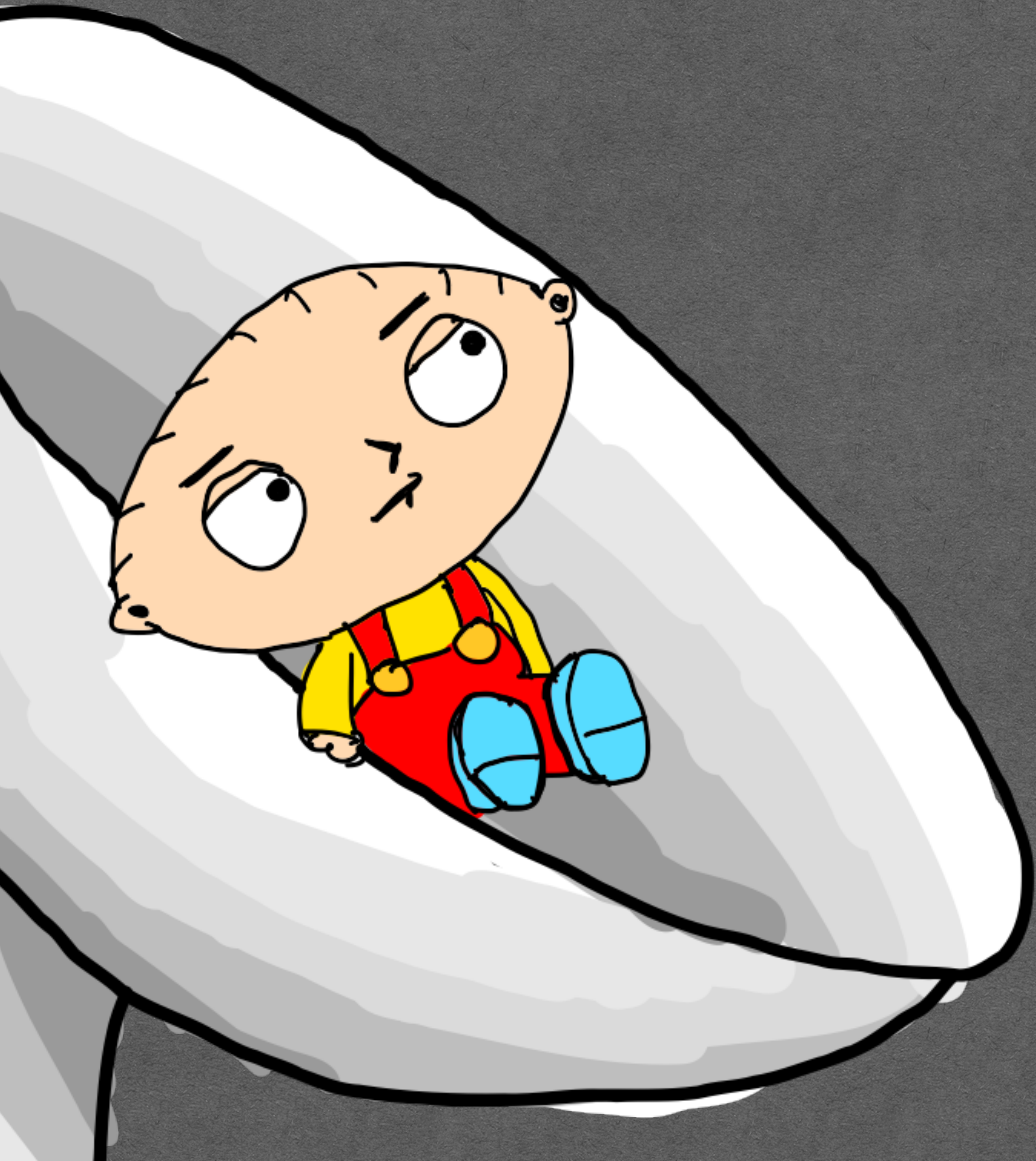
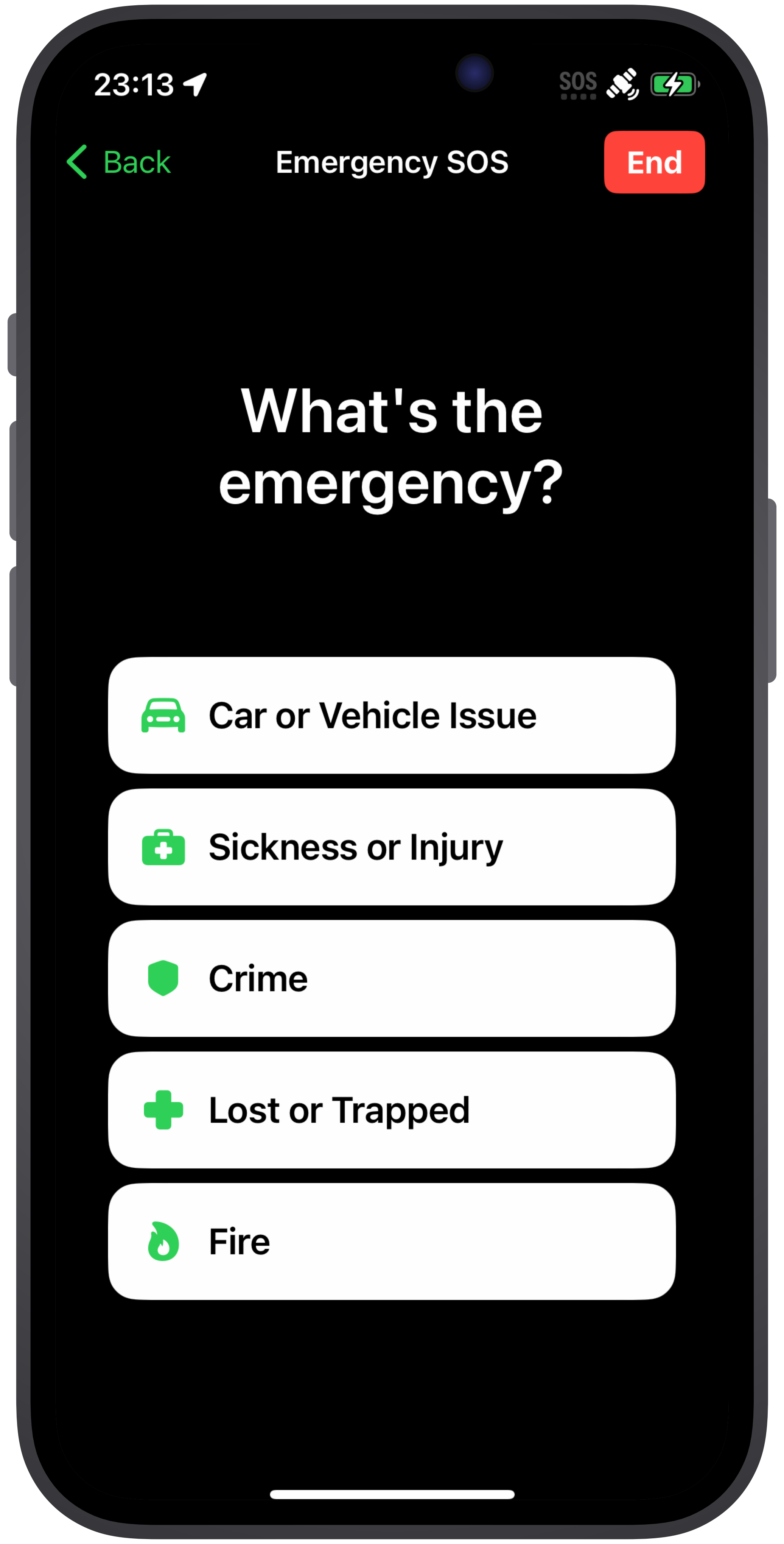
# Starshields for iOS

## Navigating the Security Cosmos in Satellite Communication



Jiska Classen*, Alexander Heinrich*,
Fabian Portner, Felix Rohrbach, Matthias Hollick

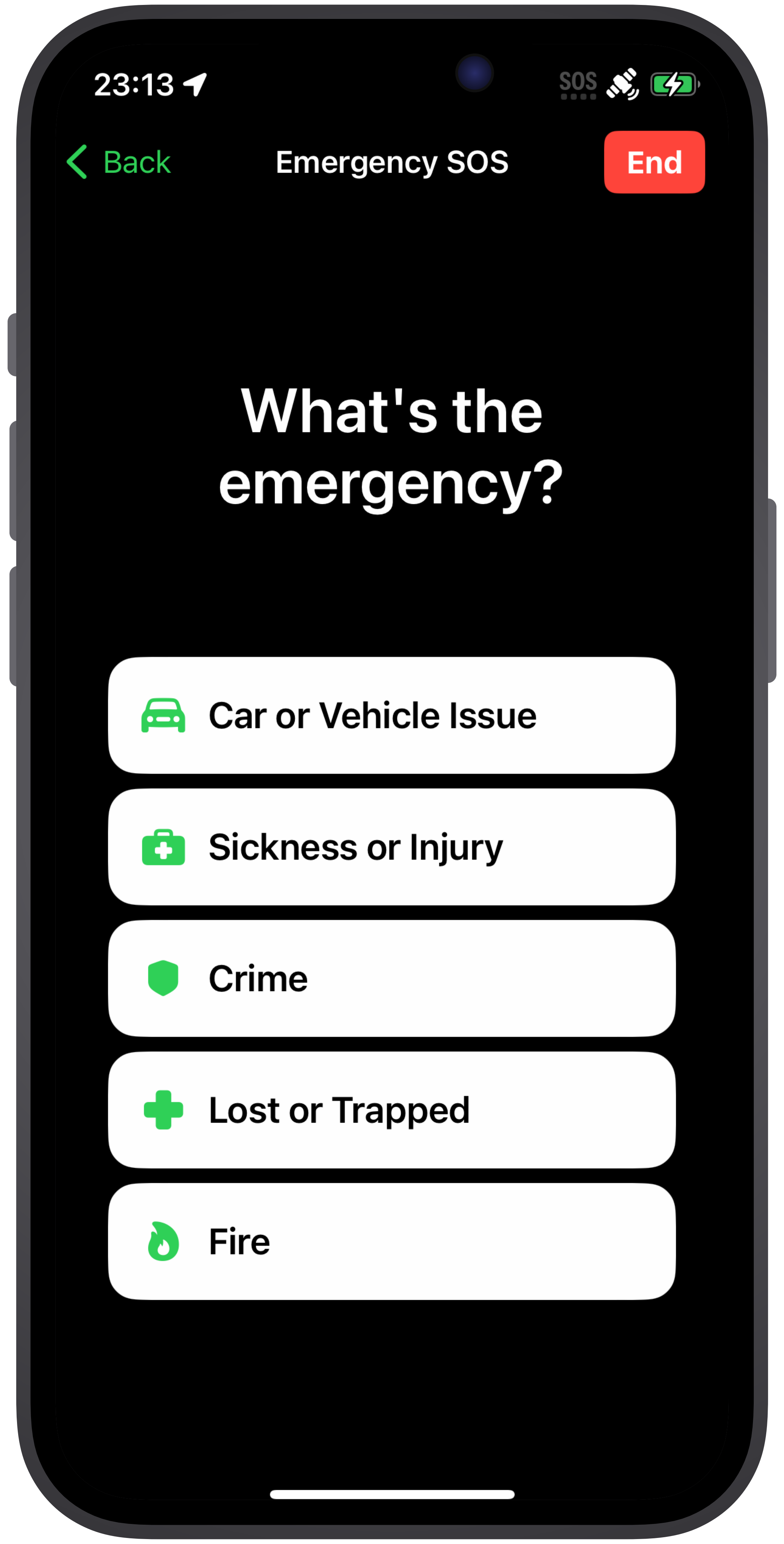
# Satellite Features



What's the emergency?

Emergency SOS

# Satellite Features



23:13

SOS

Back

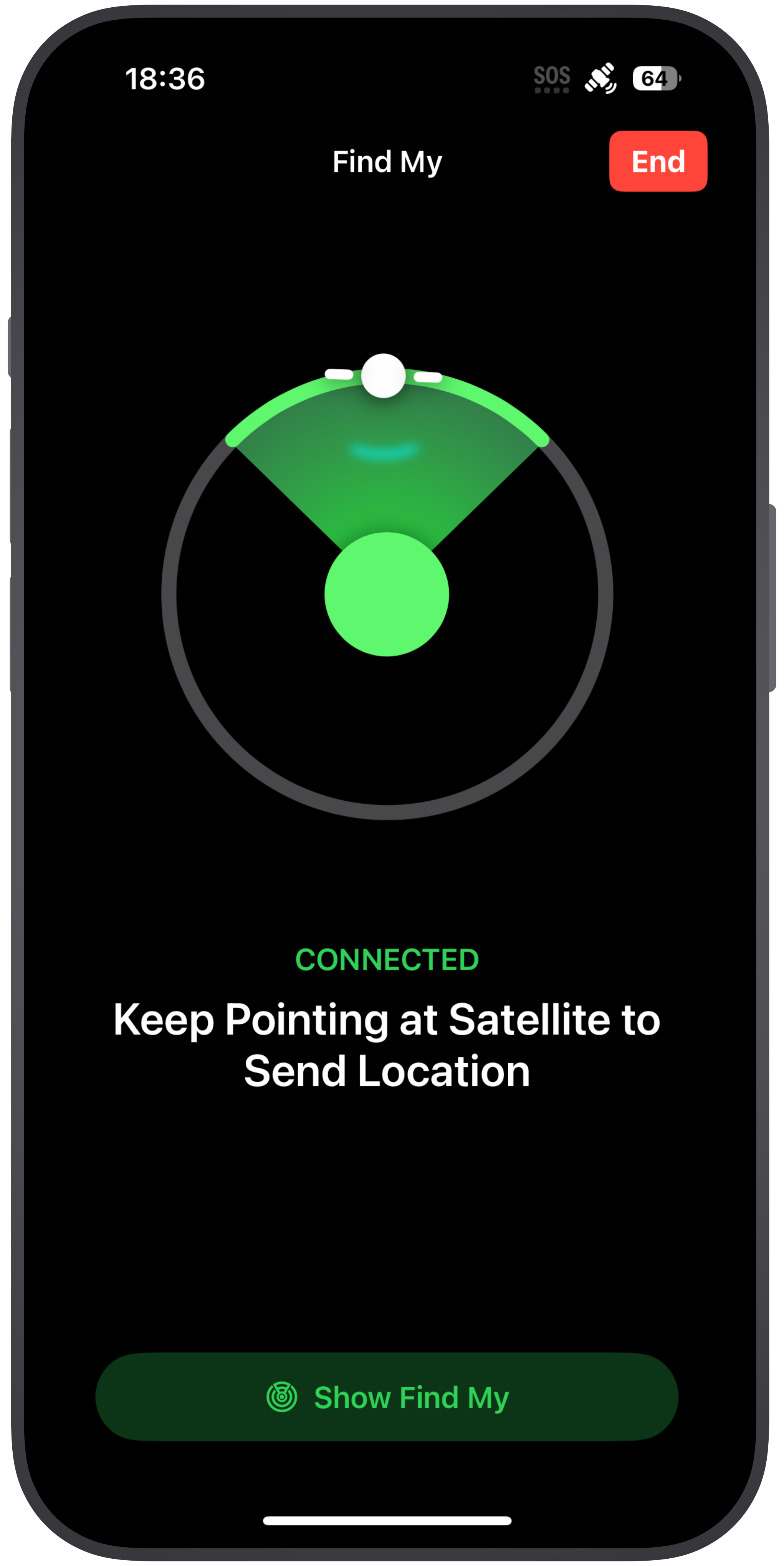
Emergency SOS

End

What's the emergency?

- Car or Vehicle Issue
- Sickness or Injury
- Crime
- Lost or Trapped
- Fire

Emergency SOS



18:36

SOS

64

Find My

End

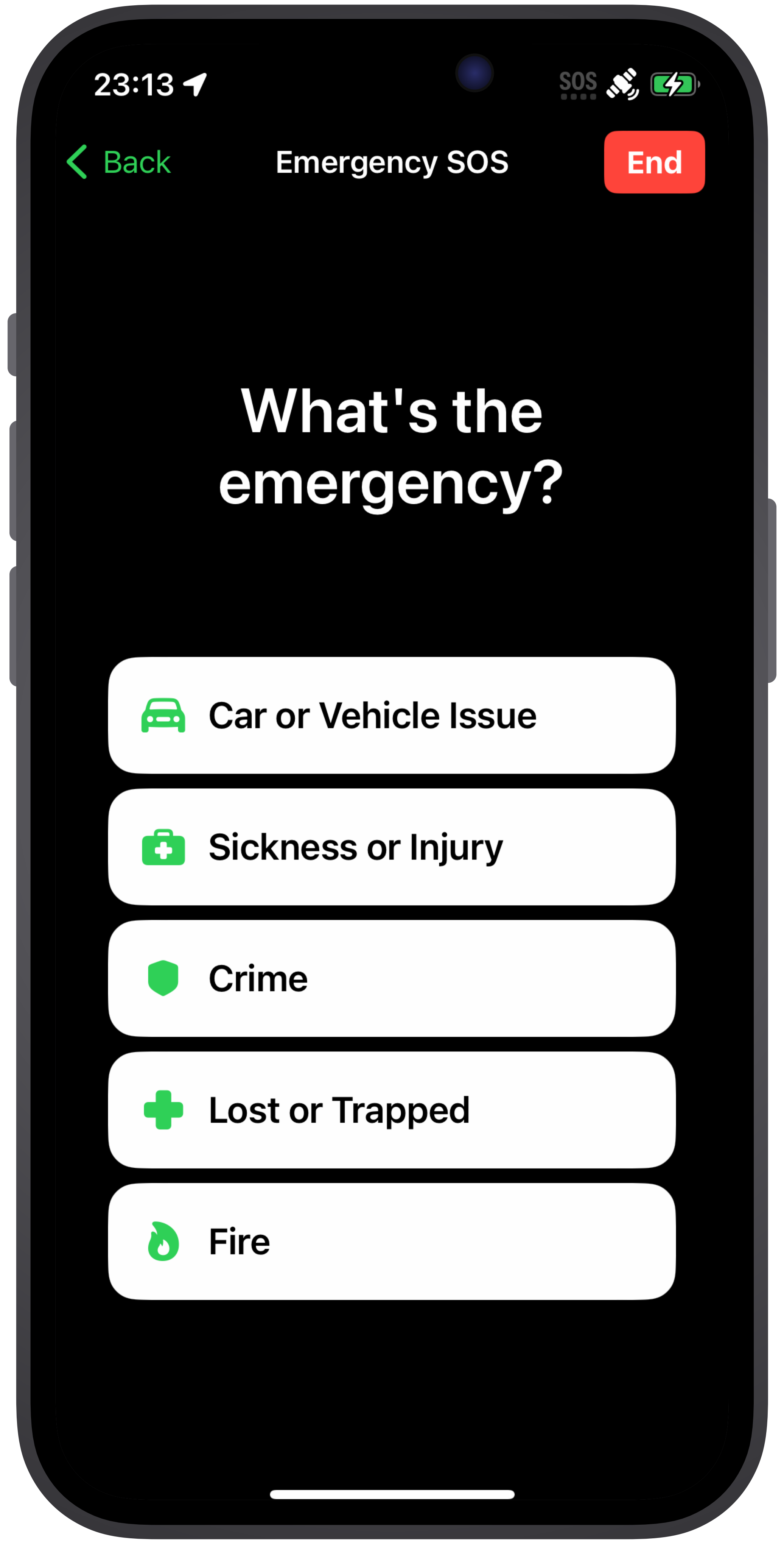
CONNECTED

Keep Pointing at Satellite to Send Location

Show Find My

Find My Friends

# Satellite Features



23:13

SOS

Back

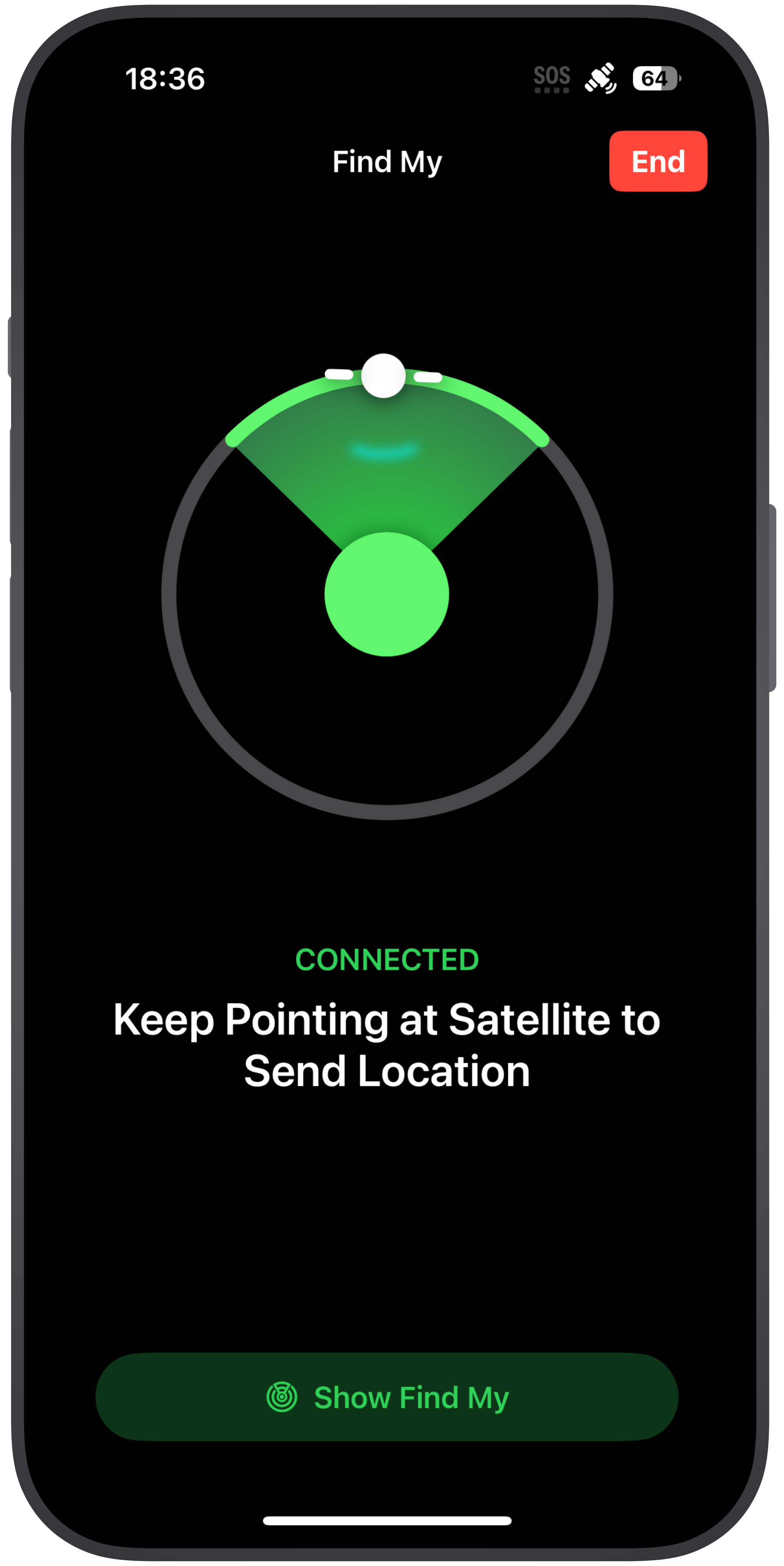
Emergency SOS

End

What's the emergency?

- Car or Vehicle Issue
- Sickness or Injury
- Crime
- Lost or Trapped
- Fire

Emergency SOS



18:36

SOS 64

Find My

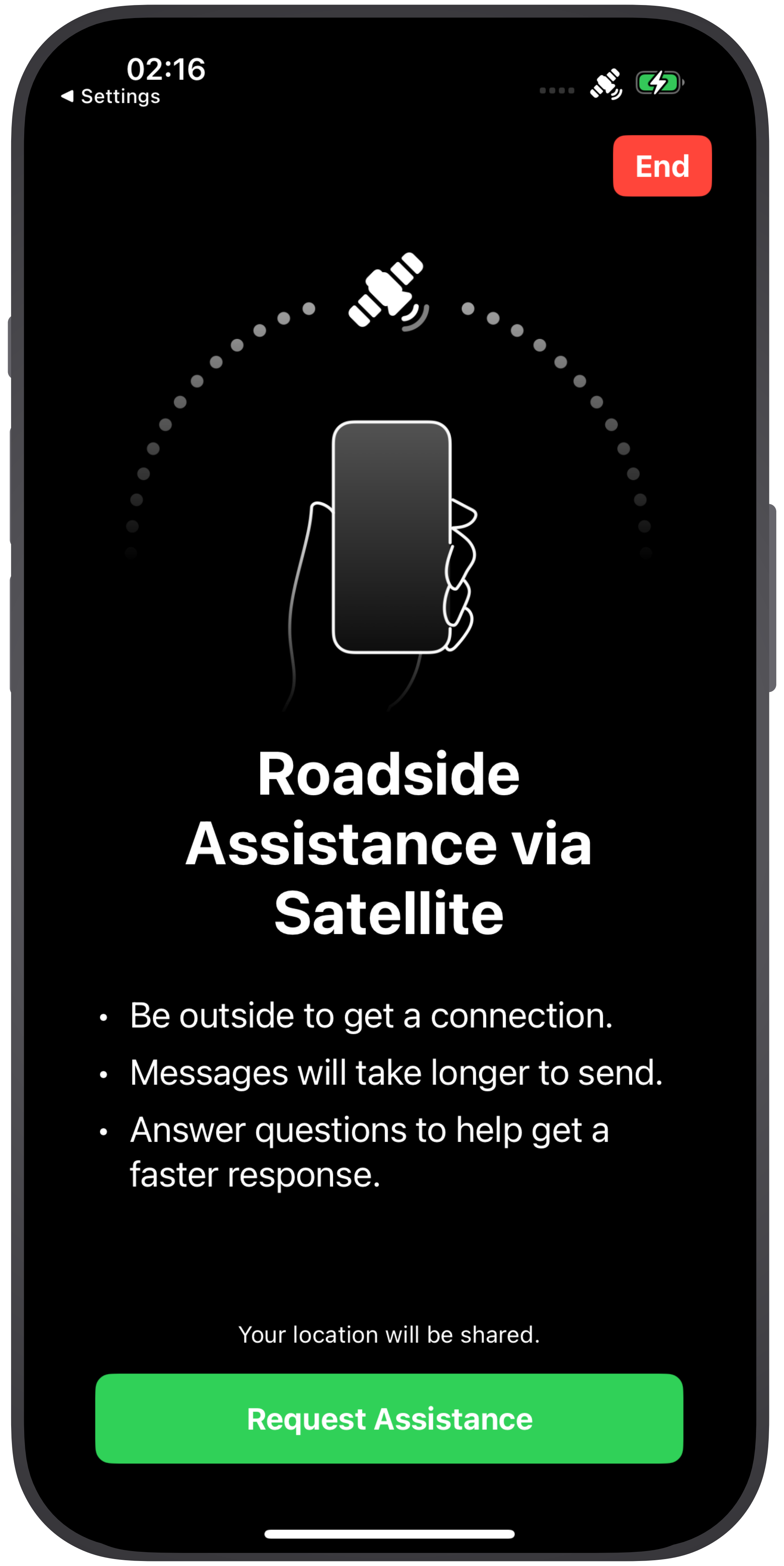
End

CONNECTED

Keep Pointing at Satellite to Send Location

Show Find My

Find My Friends



02:16

◂ Settings

End

Roadside Assistance via Satellite

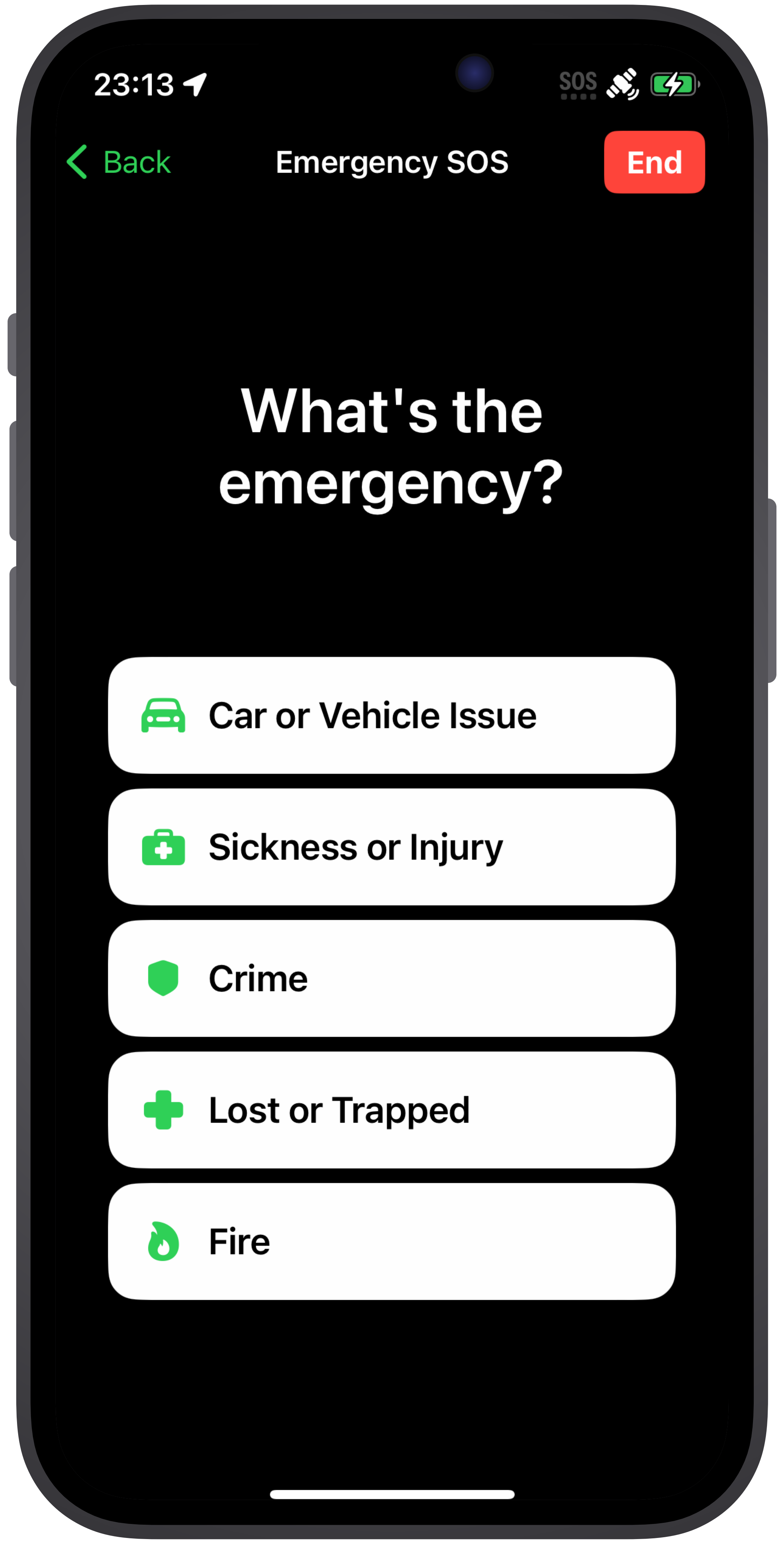
- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

Your location will be shared.

Request Assistance

Roadside Assistance

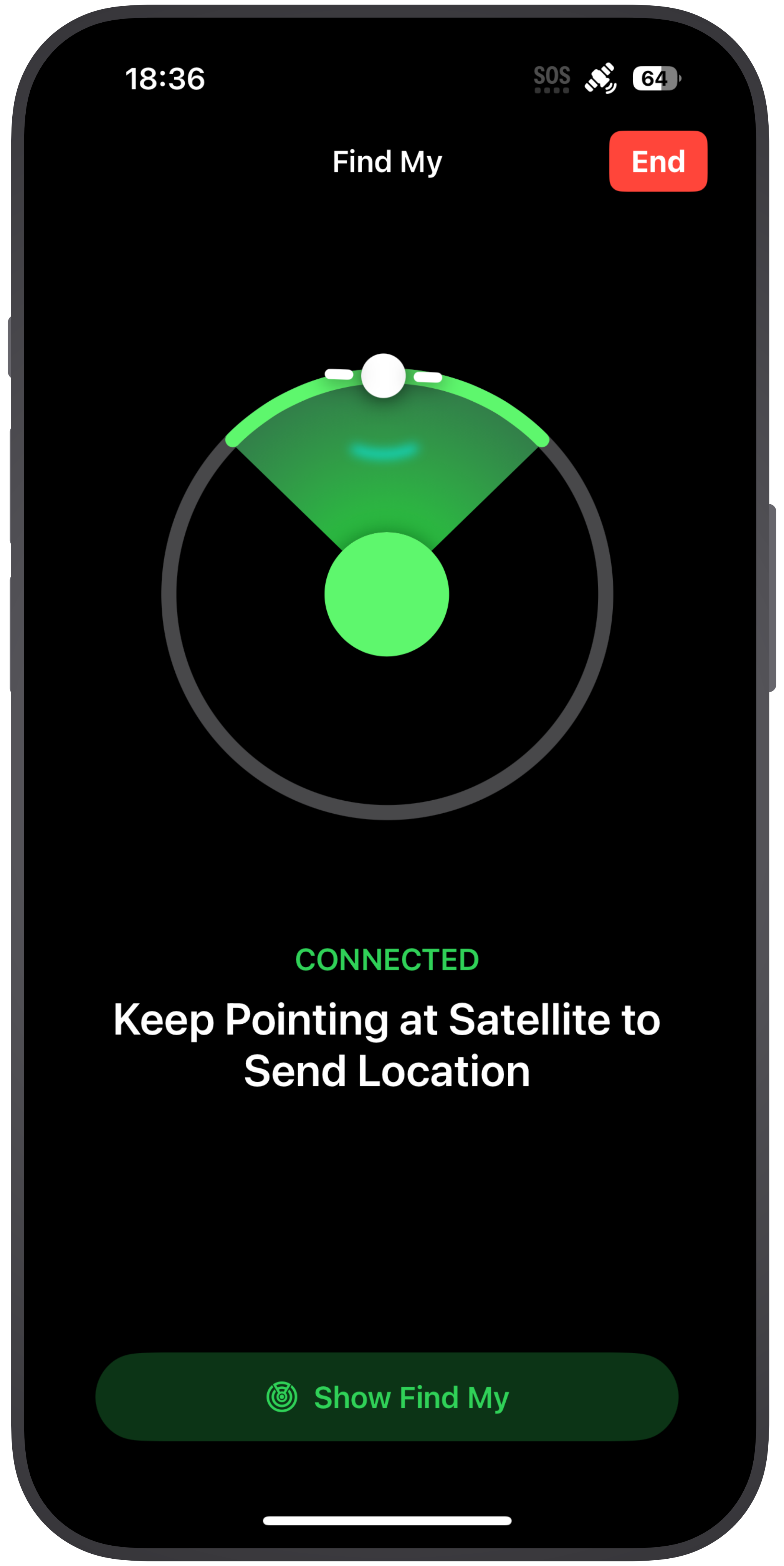
# Satellite Features



What's the emergency?

- Car or Vehicle Issue
- Sickness or Injury
- Crime
- Lost or Trapped
- Fire

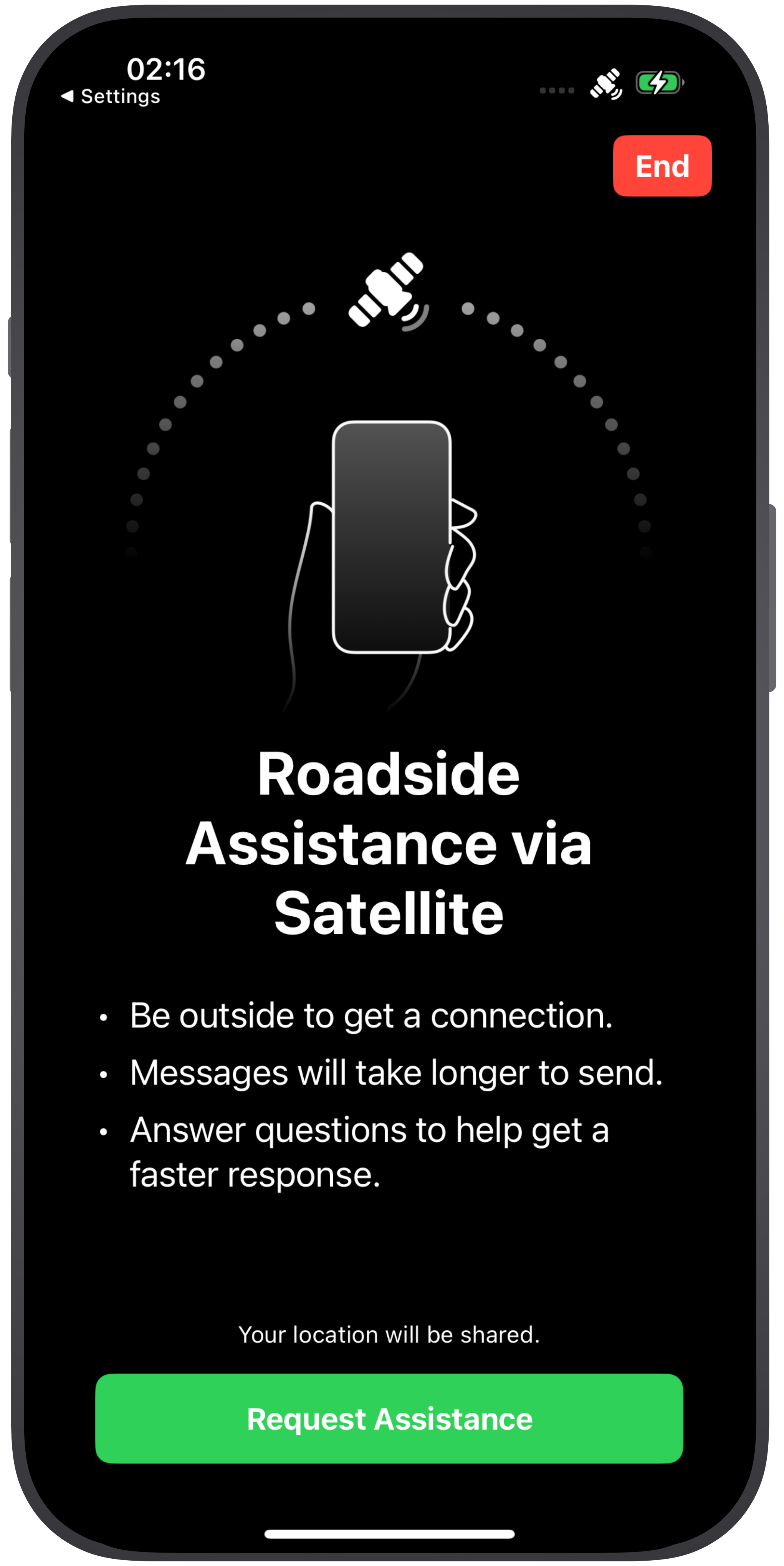
Emergency SOS



CONNECTED

Keep Pointing at Satellite to Send Location

Find My Friends



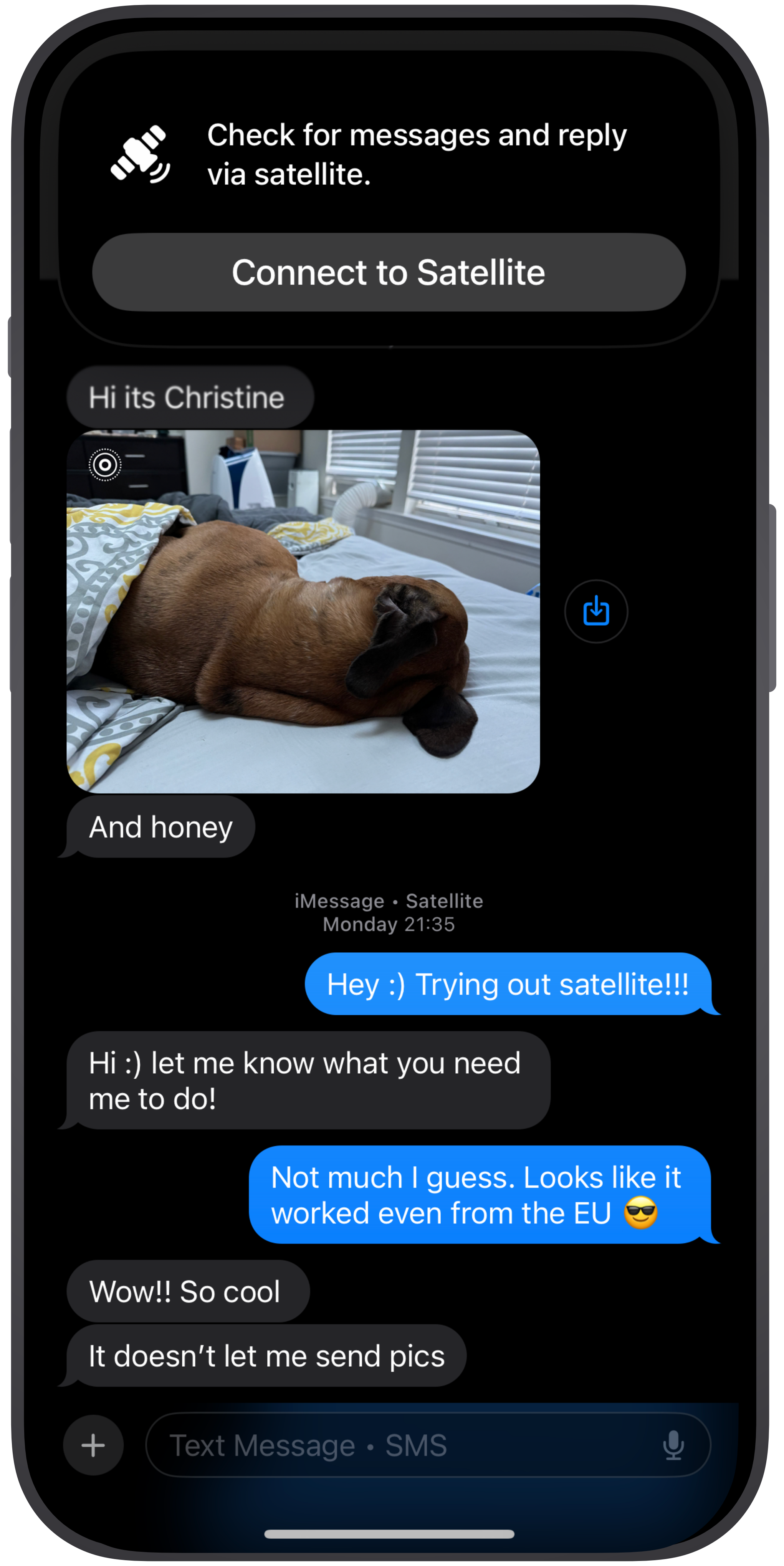
Roadside Assistance via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

Your location will be shared.

Request Assistance

Roadside Assistance


Check for messages and reply via satellite.

Connect to Satellite

Hi its Christine

And honey

iMessage • Satellite
Monday 21:35

Hey :) Trying out satellite!!!

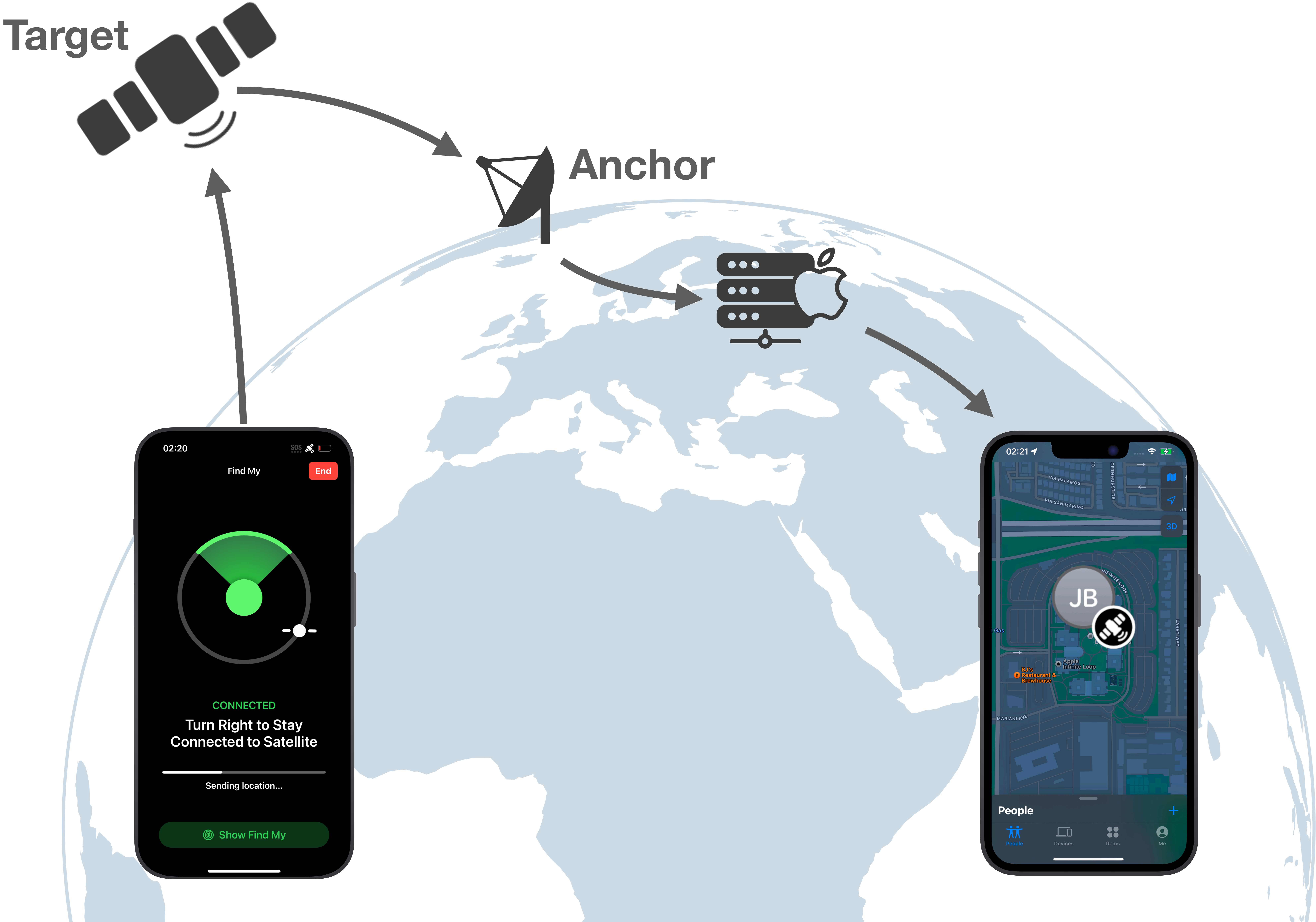
Hi :) let me know what you need me to do!

Not much I guess. Looks like it worked even from the EU 😎

Wow!! So cool

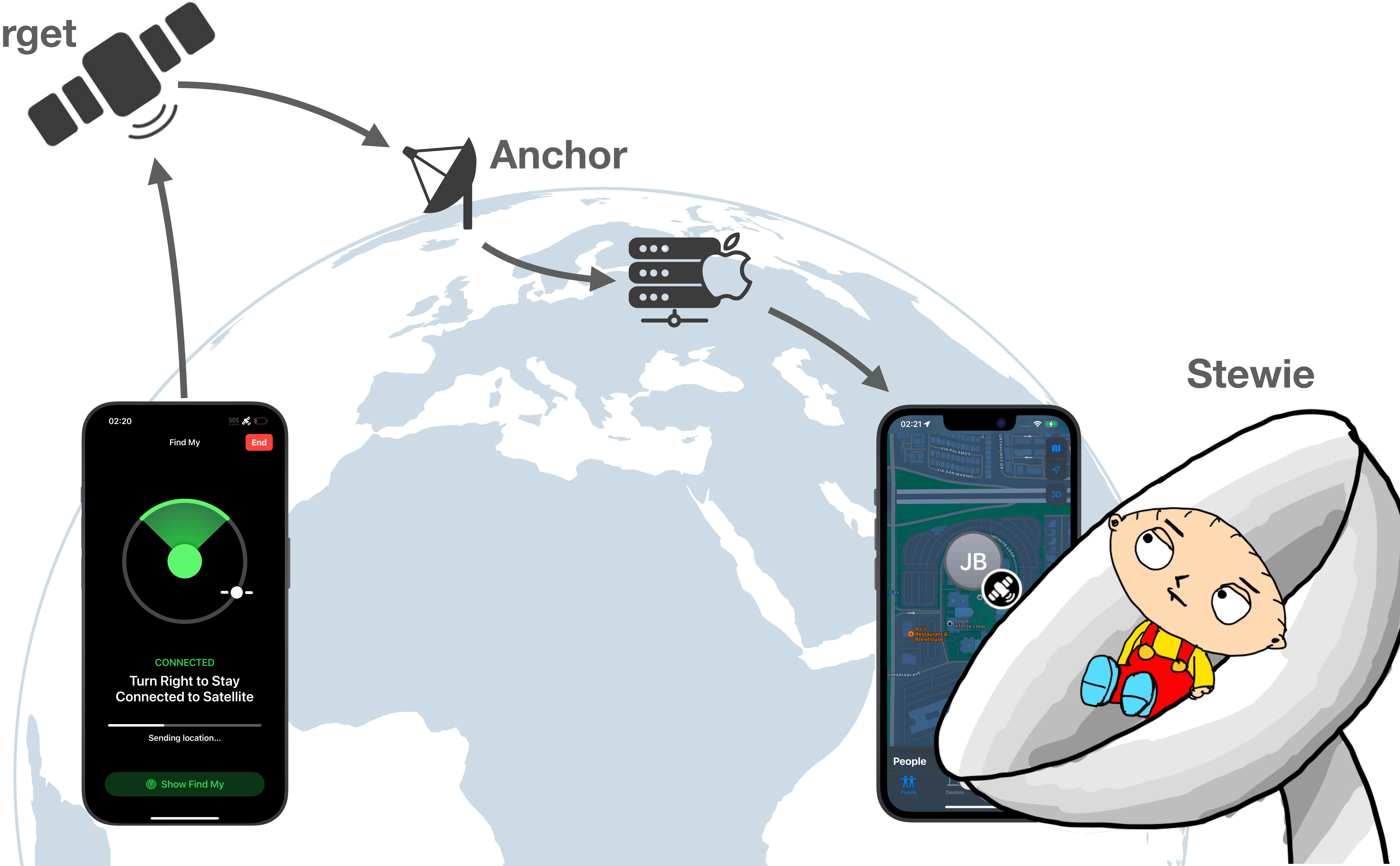
It doesn't let me send pics

Messages



Target

Anchor

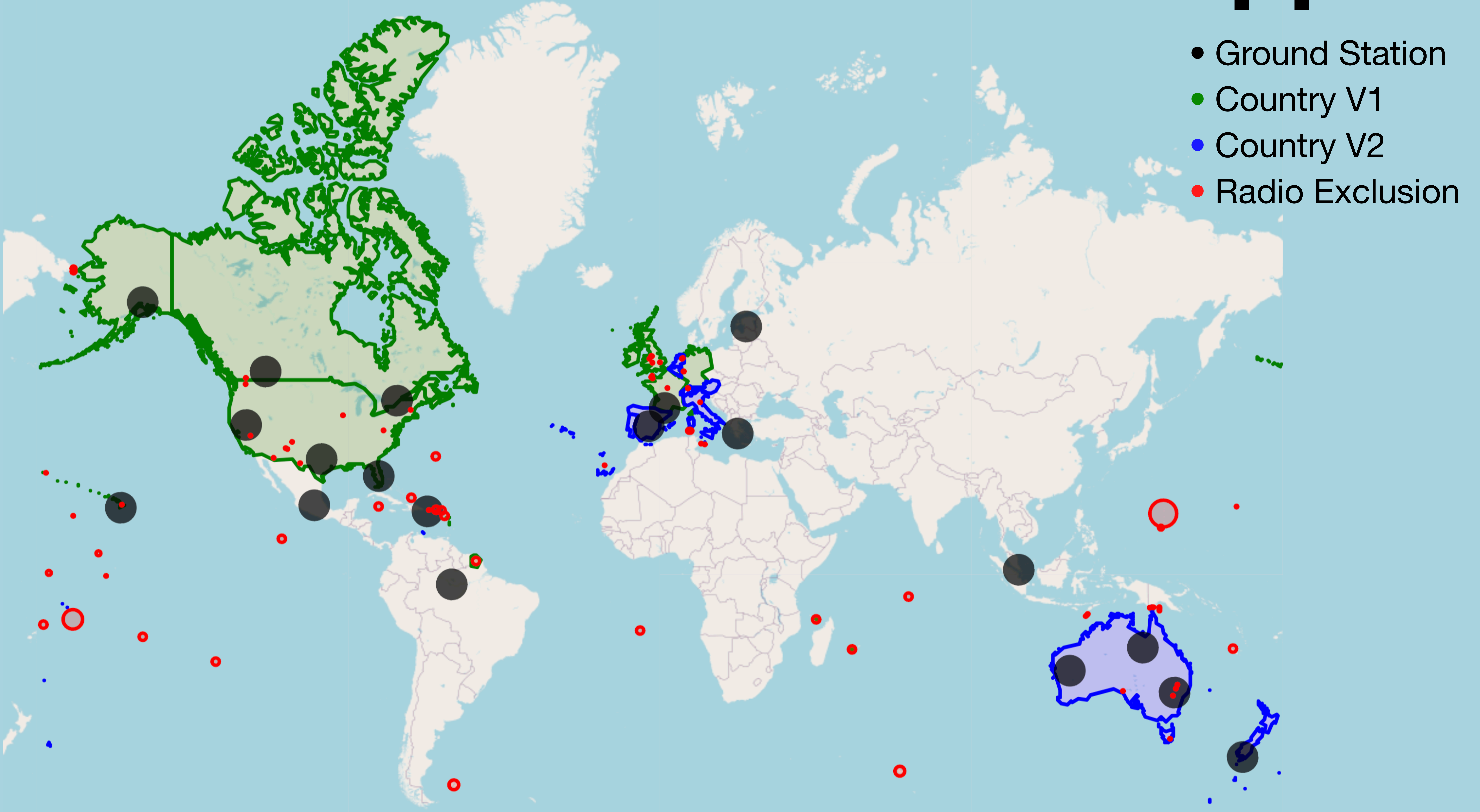


Target

Anchor

Stewie

# Globalstar Infrastructure @ Apple



# Research Questions

**RQ1**

How are security and privacy features implemented in this resource-constrained satellite communication environment?

**RQ2**

Can users bypass service restrictions imposed by Apple?

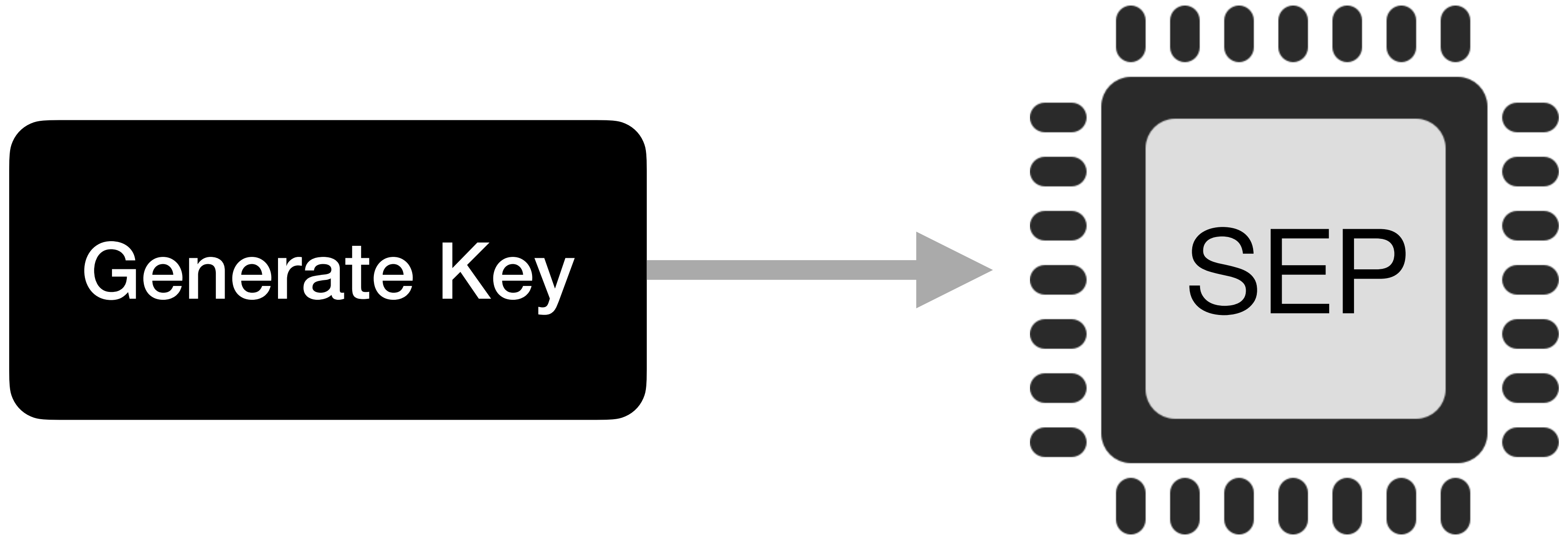
# Satellite Connectivity

# LLC Keys

# LLC Keys

Generate Key

# LLC Keys

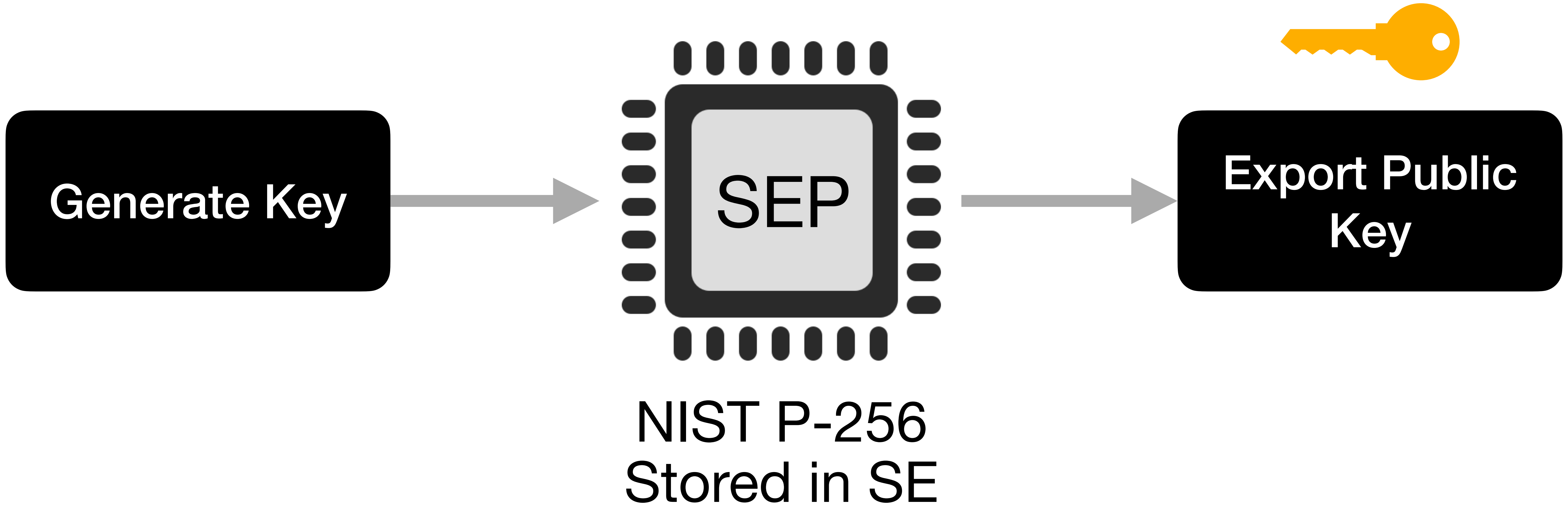


Generate Key

SEP

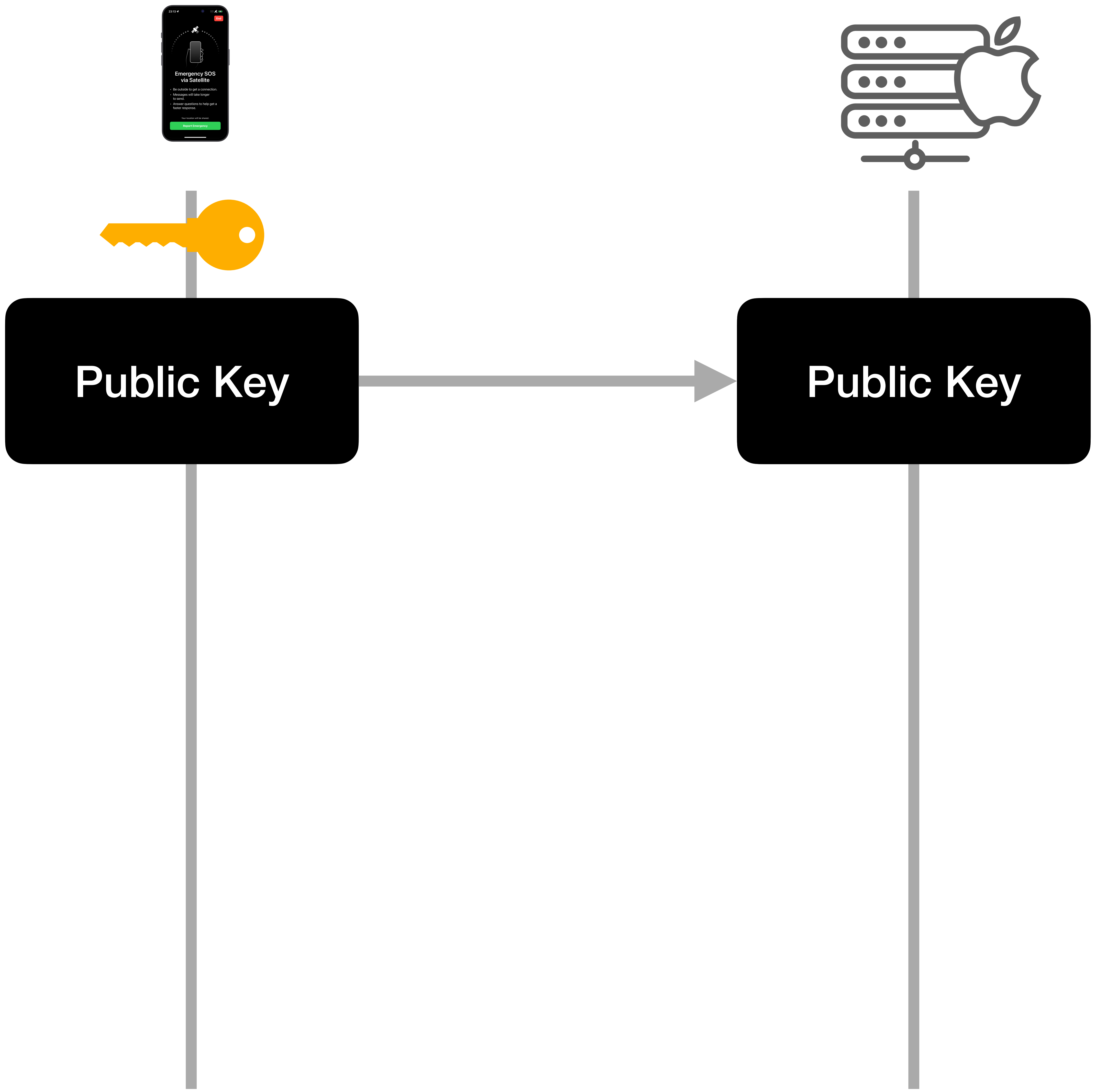
NIST P-256
Stored in SE

# LLC Keys

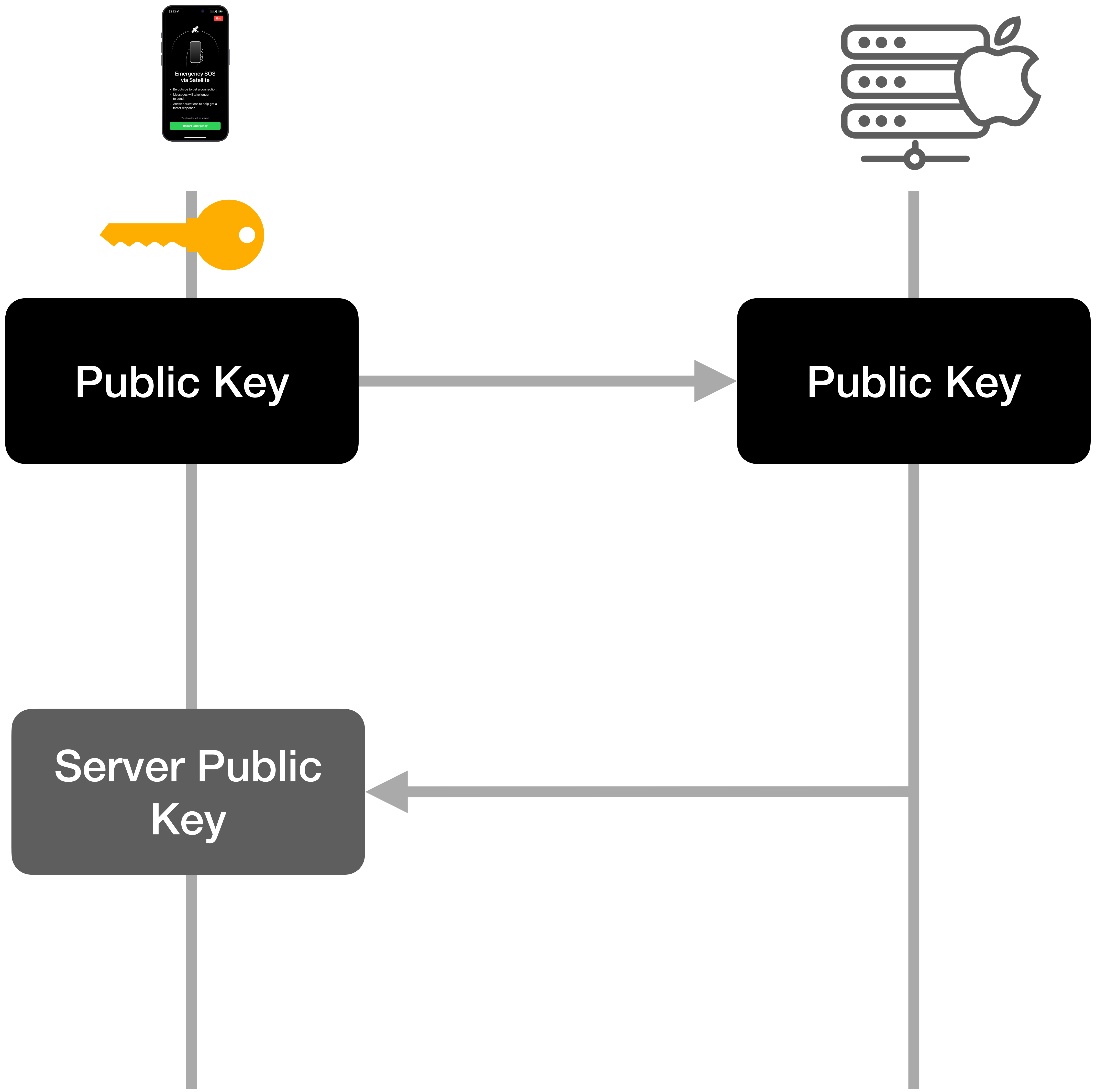


During initial Stewie provisioning (online), there are multiple LLC keys set up for satellite connections between Apple and the iPhone.

# Key Synchronisation



# Key Synchronisation



Apple remembers your public key & the server key they used for the answer.

# Session Key

23:13

SOS

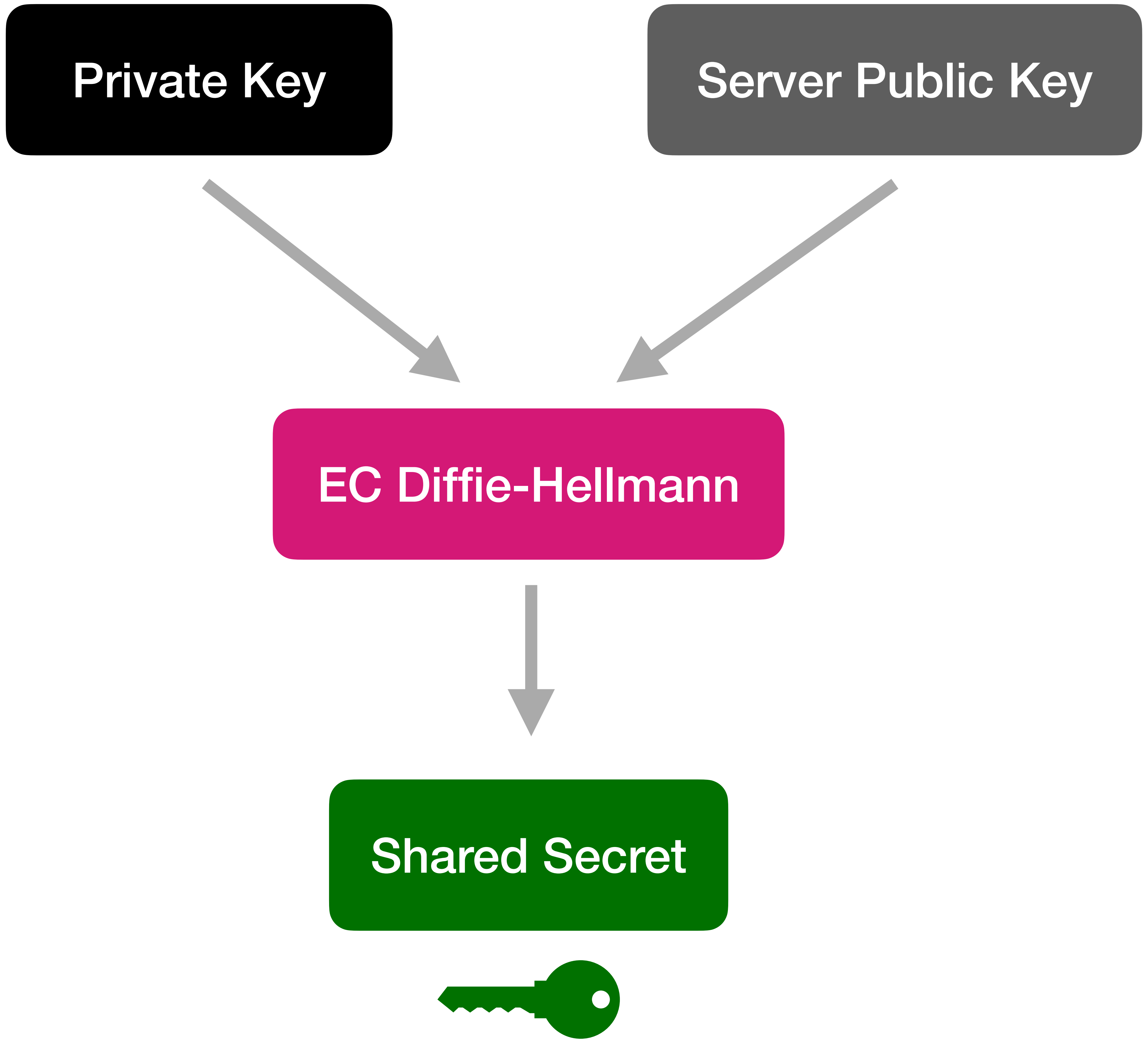
End

Emergency SOS via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

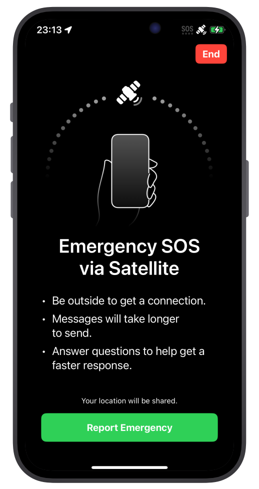
Your location will be shared.

Report Emergency



Unlike classic ECDH key exchange, we got all the keys in advance. The *shared secret* can be generated **offline** without any Internet connection!

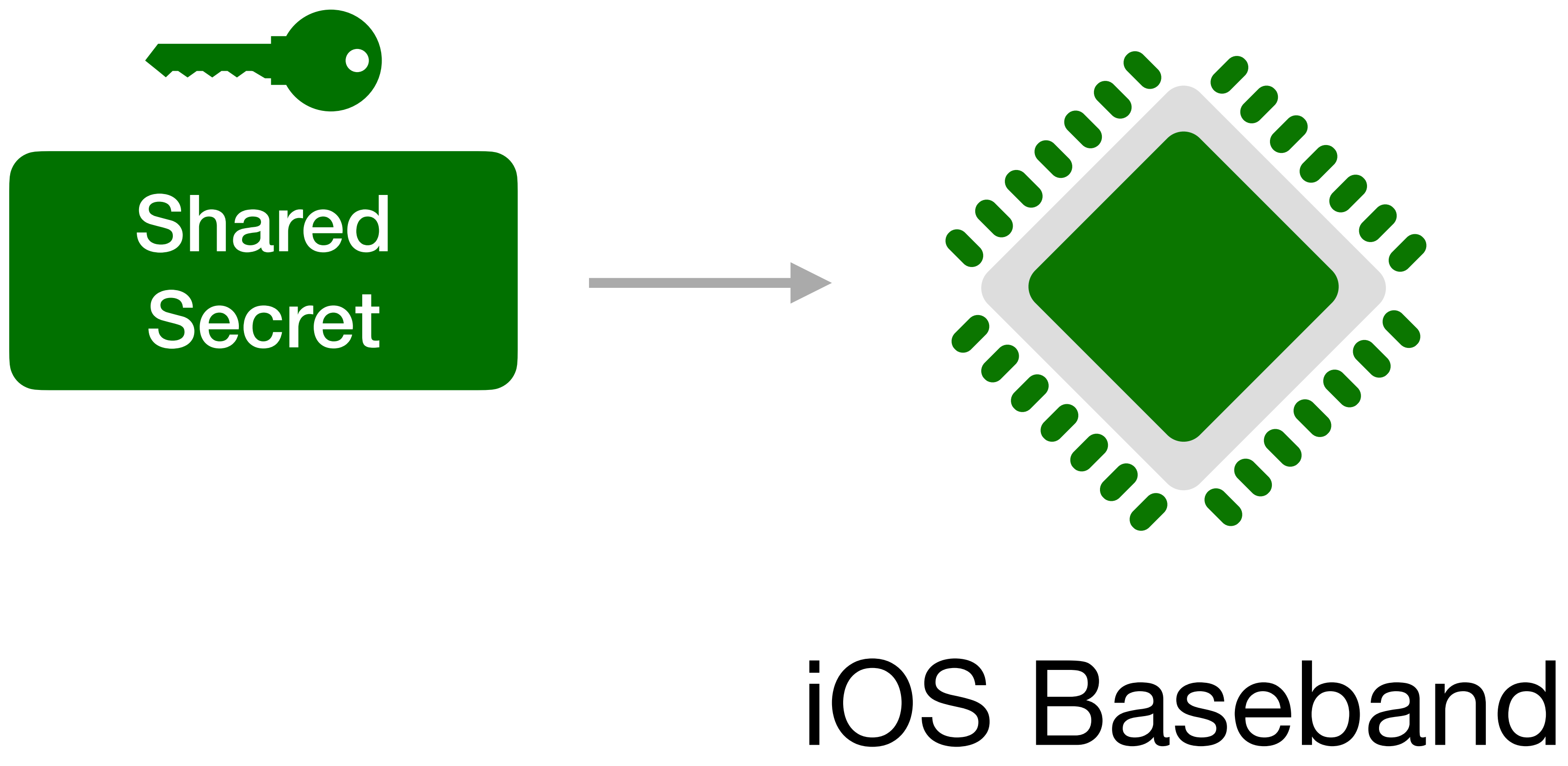
# Connect and Authenticate



Emergency SOS via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

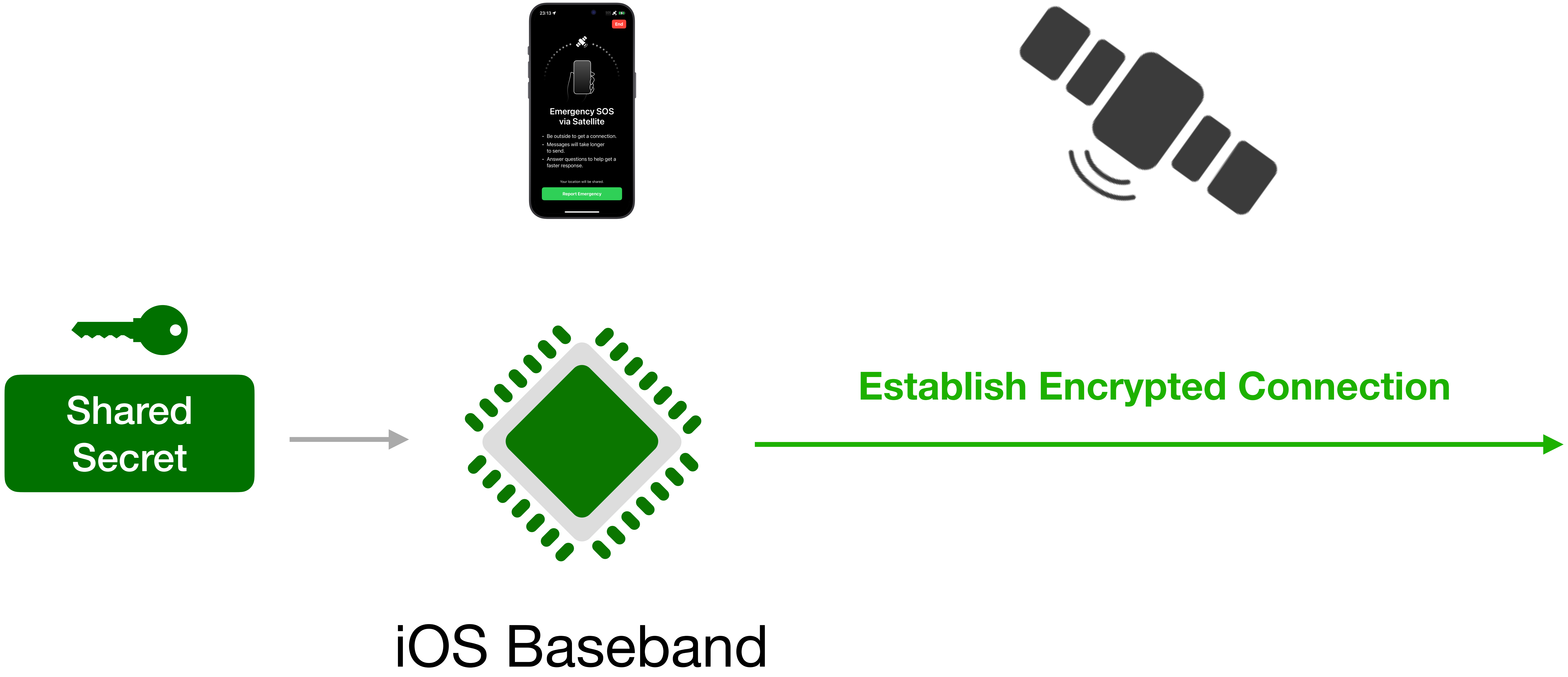
Your location will be shared.



Shared Secret

iOS Baseband

# Connect and Authenticate



Emergency SOS via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

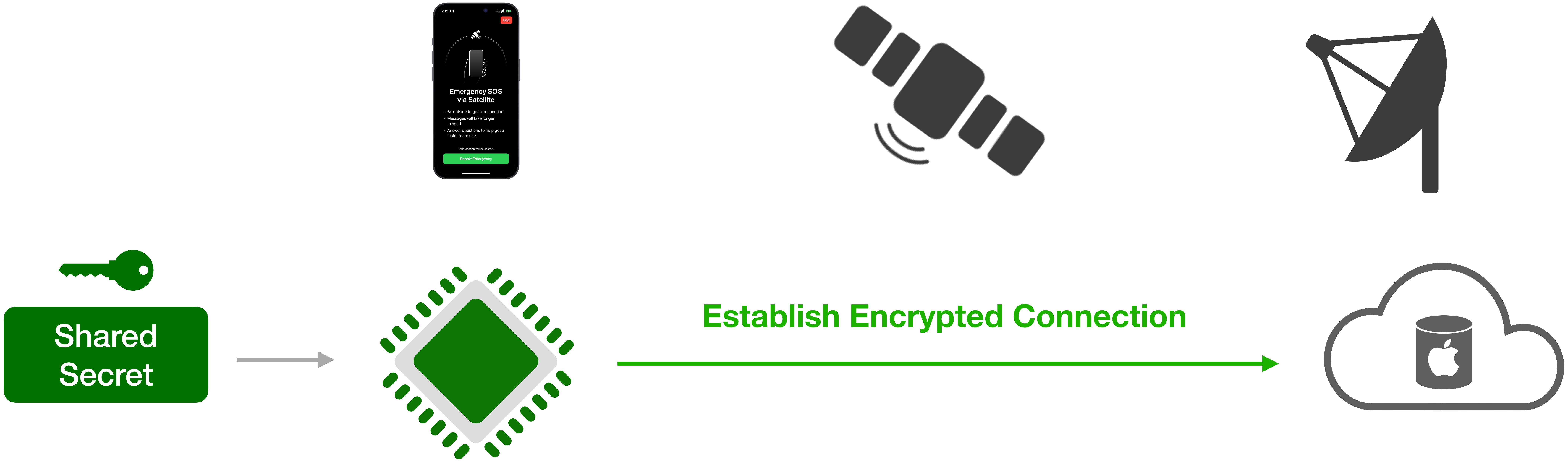
Your location will be shared.

Shared Secret

iOS Baseband

Establish Encrypted Connection

# Connect and Authenticate



23:13

SOS

End

Emergency SOS via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

Your location will be shared.

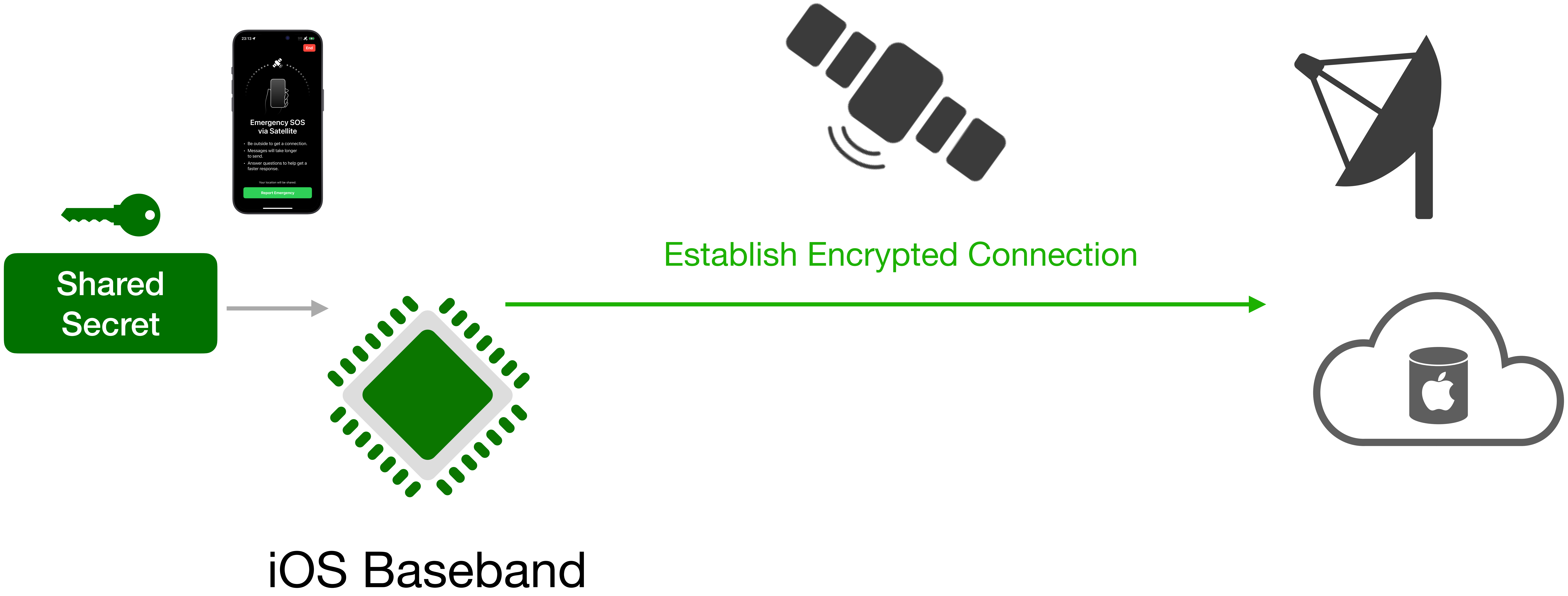
Report Emergency

Shared Secret

Establish Encrypted Connection

iOS Baseband

# Emergency SOS Encryption Keys

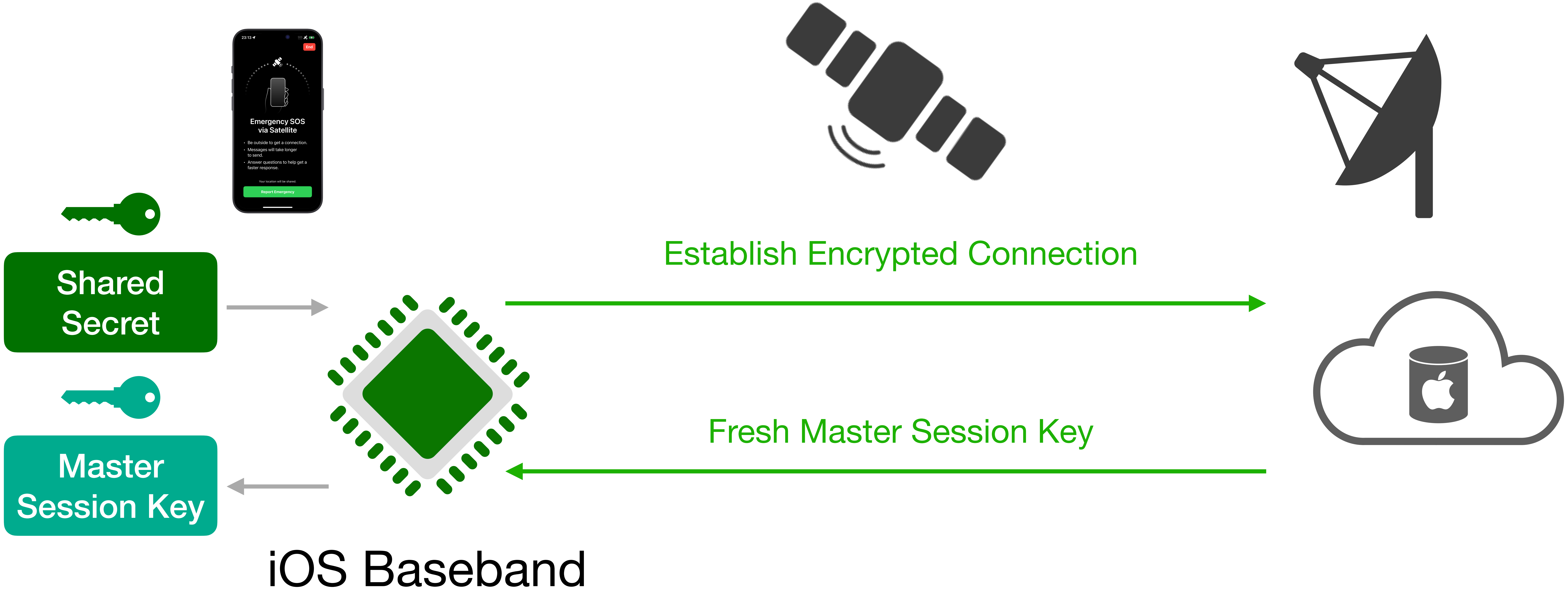


**Emergency SOS via Satellite**

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

Your location will be shared.

# Emergency SOS Encryption Keys



Emergency SOS via Satellite

- Be outside to get a connection.
- Messages will take longer to send.
- Answer questions to help get a faster response.

Your location will be shared.

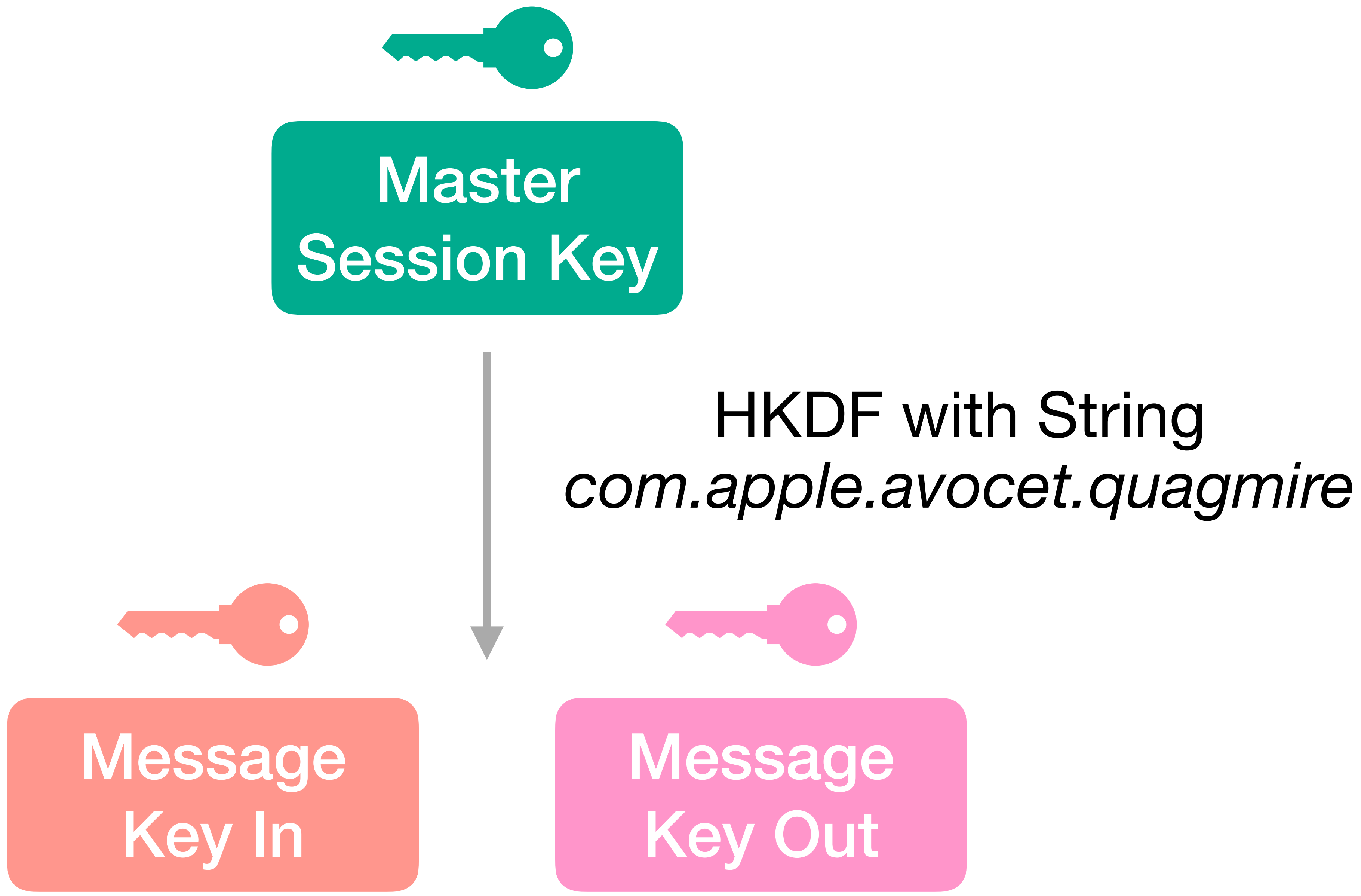
# Text Encryption

# Text Encryption

Master Session Key

# Text Encryption

Using a Hashed Key Derivation Function, we can use one 256 bit key to create two 256 bit keys!



Master Session Key

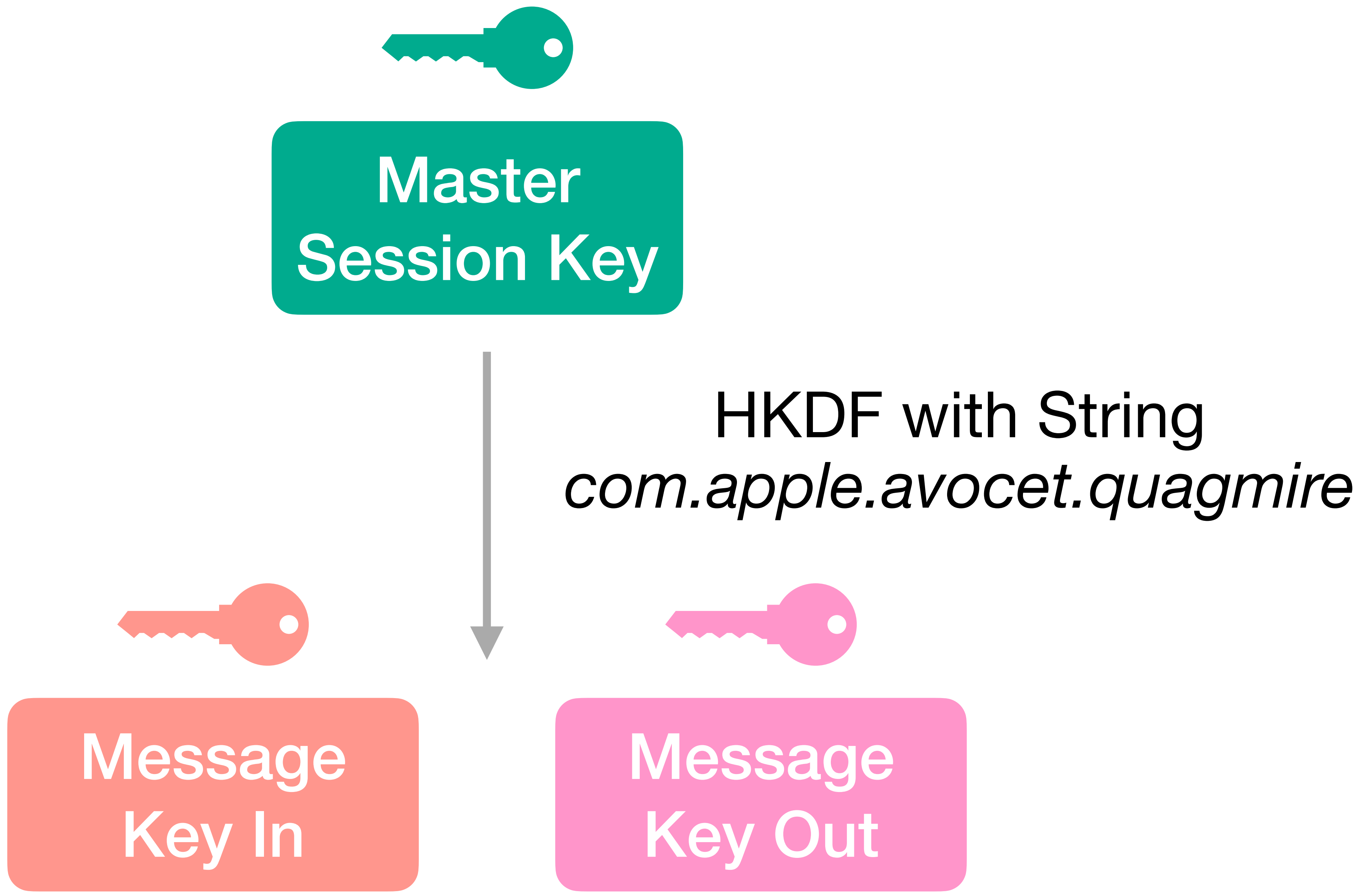
HKDF with String *com.apple.avocet.quagmire*

Message Key In

Message Key Out

# Text Encryption

Using a Hashed Key Derivation Function, we can use one 256 bit key to create two 256 bit keys!



Master Session Key

HKDF with String *com.apple.avocet.quagmire*

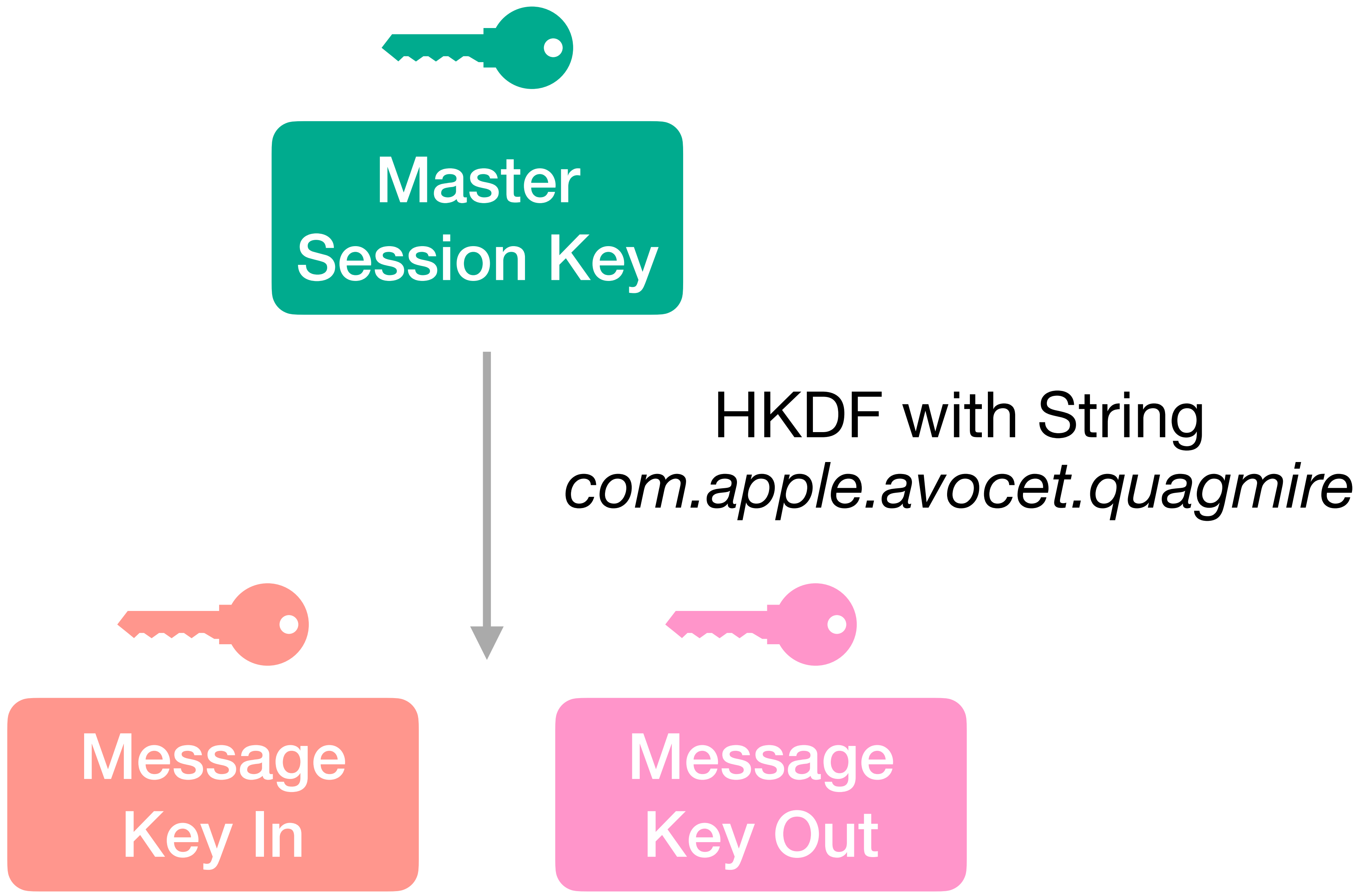
Message Key In

Message Key Out

| | | | |
|---|---|---|---|
| Text Message<br>*Type=0x02* | Conversation ID<br>*Incrementing* | Message ID<br>*Incrementing* | Compressed Text |

# Text Encryption

Using a Hashed Key Derivation Function, we can use one 256 bit key to create two 256 bit keys!

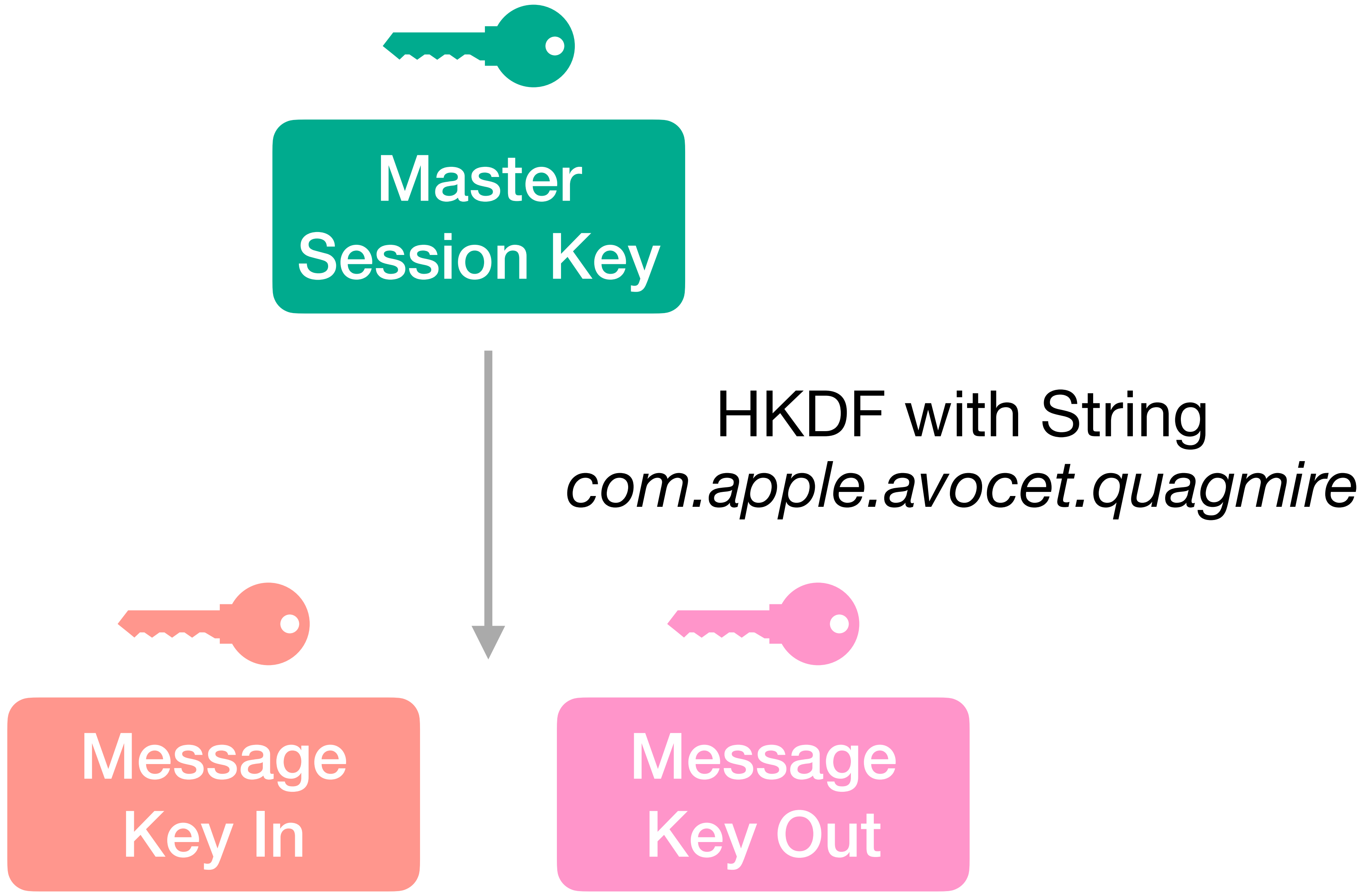


IV

| | | | |
|---|---|---|---|
| Text Message<br>*Type=0x02* | Conversation ID<br>*Incrementing* | Message ID<br>*Incrementing* | Compressed Text |

# Text Encryption

Using a Hashed Key Derivation Function, we can use one 256 bit key to create two 256 bit keys!



Master Session Key

HKDF with String
*com.apple.avocet.quagmire*

Message Key In

Message Key Out

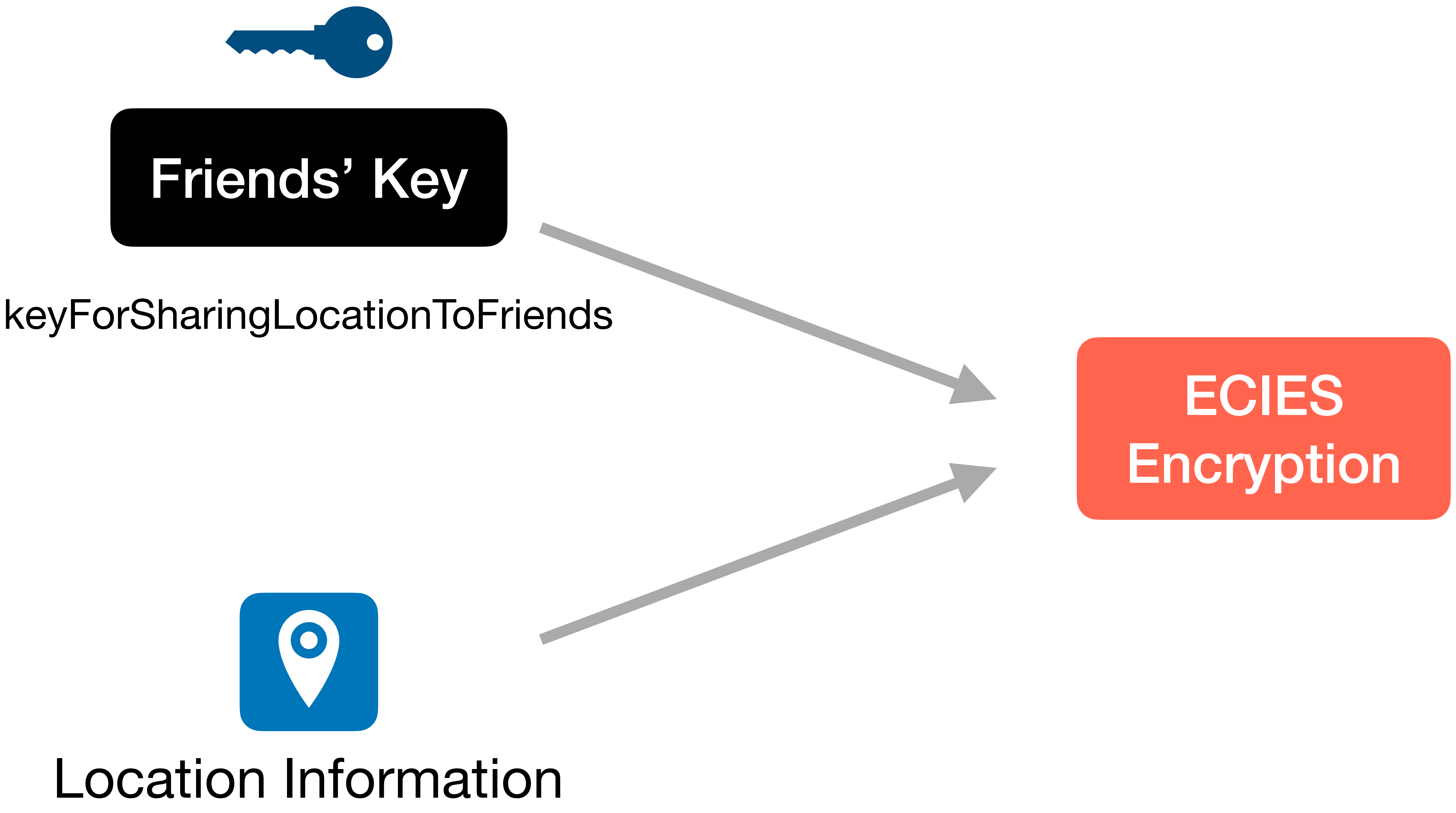
IV

AES CTR Mode

| | | | |
|---|---|---|---|
| Text Message<br>*Type=0x02* | Conversation ID<br>*Incrementing* | Message ID<br>*Incrementing* | 🔒 Compressed Text |

# End-to-End Location Encryption

# End-to-End Location Encryption



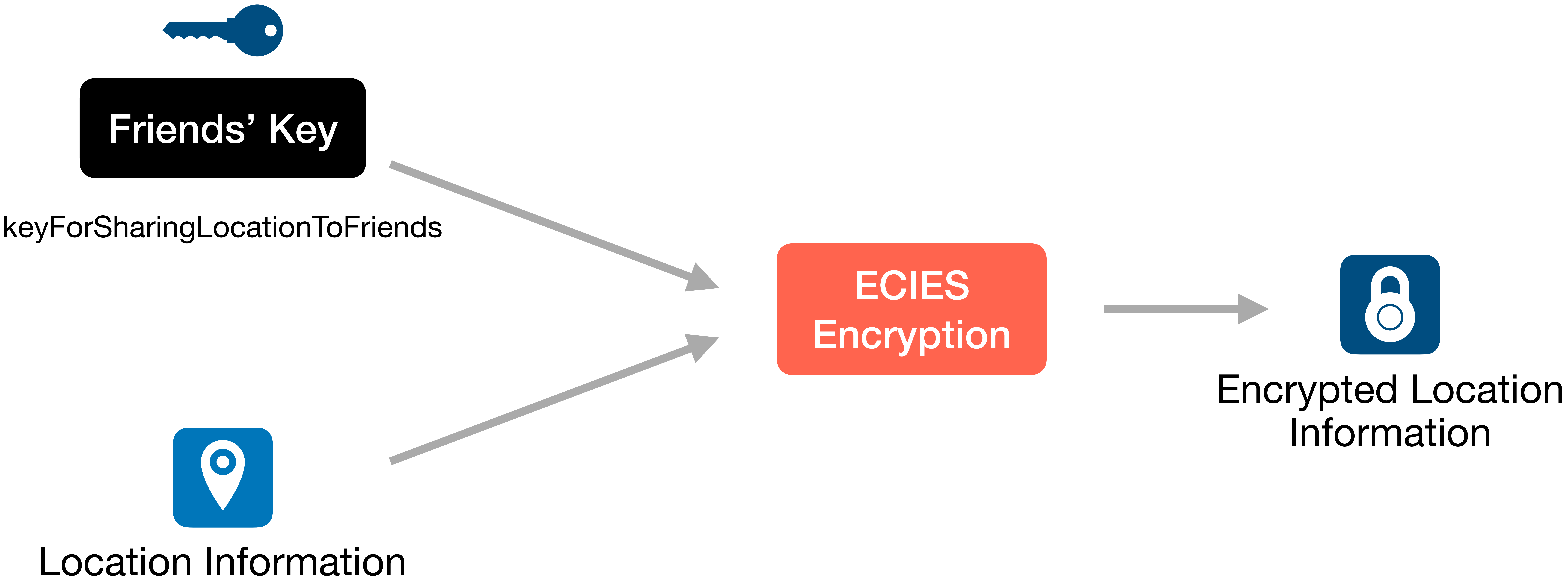
Friends’ Key

keyForSharingLocationToFriends

ECIES Encryption

Location Information

# End-to-End Location Encryption



Friends' Key

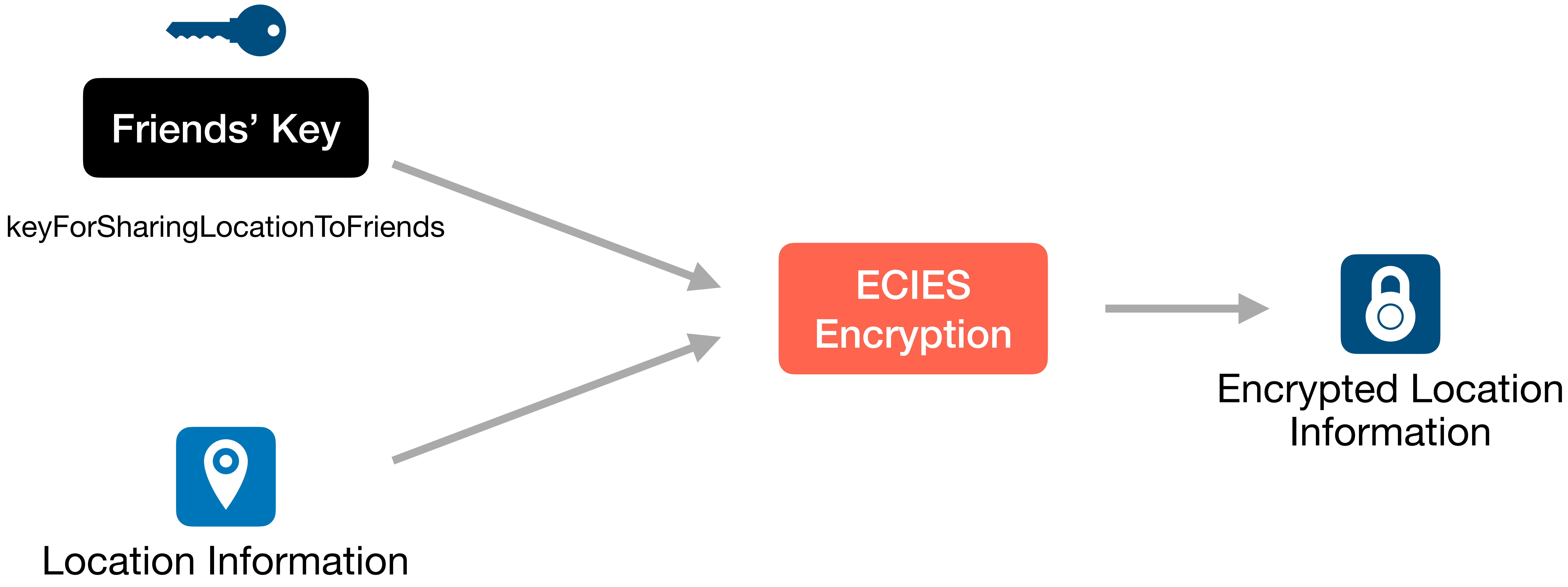
keyForSharingLocationToFriends

Location Information

ECIES Encryption

Encrypted Location Information

# End-to-End Location Encryption



Friends' Key

keyForSharingLocationToFriends

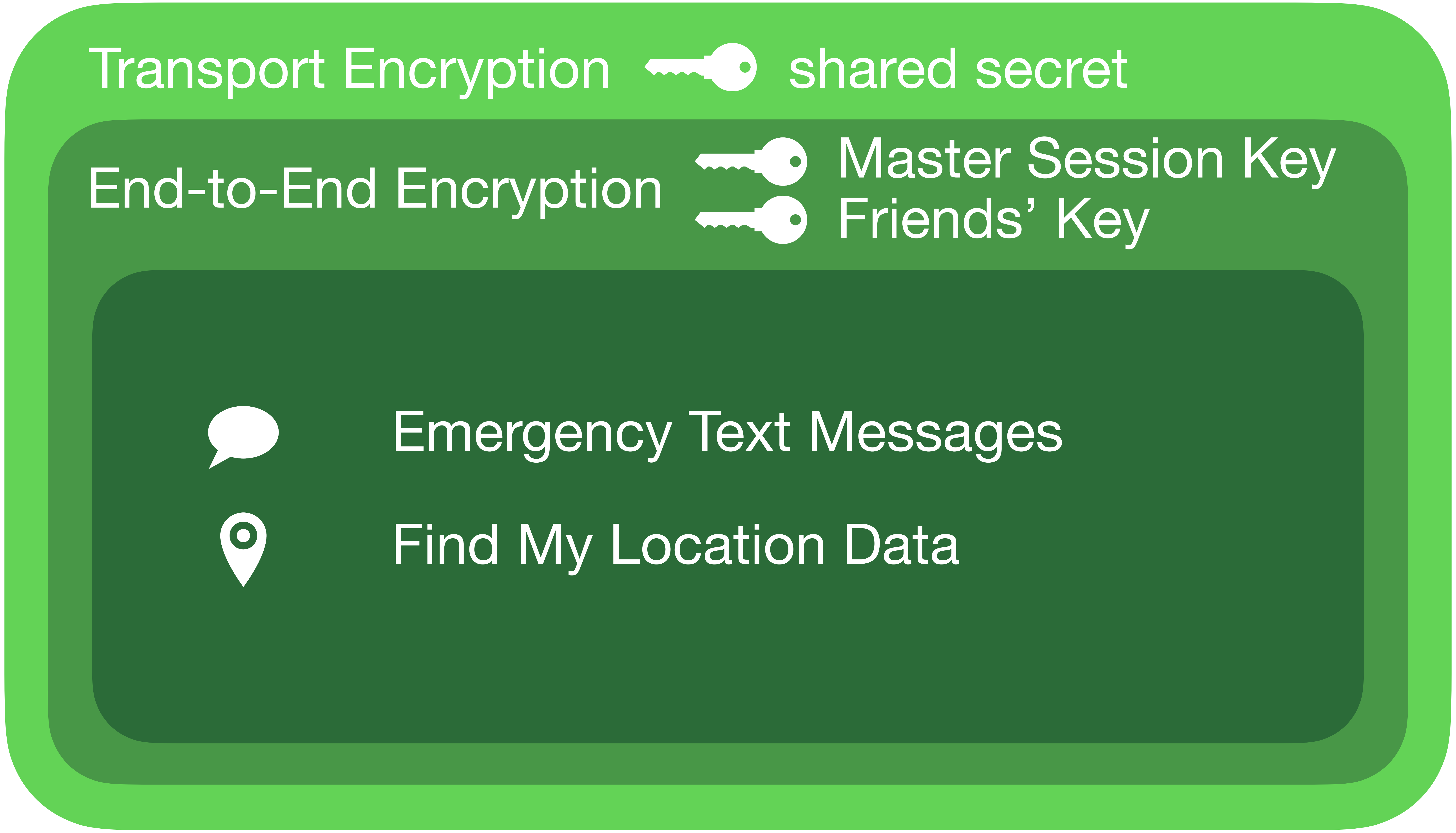
Location Information

ECIES Encryption

Encrypted Location Information

```
eciesEncryptionStandardVariableIVX963SHA256AESGCM
```

# Data Protection Mechanisms



Transport Encryption shared secret

End-to-End Encryption

Master Session Key

Friends’ Key

Emergency Text Messages

Find My Location Data

# Bypassing Restrictions

🤔🤔🤔

Globalstar offers satellite services in Poland!

```
…
<key>countries</key>
<array>
    <dict>
        <key>allowed_services</key>
        <array>
            <string>emergency</string>
            <string>findmy</string>
        </array>
        <key>fwd_alternate_channels</key>
        <array>
            <integer>262220</integer>
            <integer>262270</integer>
        </array>
        <key>fwd_channel</key>
        <integer>262170</integer>
        <key>iso3166_alpha_3</key>
        <string>DEU</string>
…
```

```
/private/var/mobile/Library/Trial/Treatments/
803/factorPacks/.../assets/Config/Config.plist
```

```
...
<key>countries</key>
<array>
    <dict>
        <key>allowed_services</key>
        <array>
            <string>emergency</string>
            <string>findmy</string>
        </array>
        <key>fwd_alternate_channels</key>
        <array>
            <integer>262220</integer>
            <integer>262270</integer>
        </array>
        <key>fwd_channel</key>
        <integer>262170</integer>
        <key>iso3166_alpha_3</key>
        <string>~~DEU~~</string>
...
```

**POL**

/private/var/mobile/Library/Trial/Treatments/803/factorPacks/.../assets/Config/Config.plist

Hohenholzer Forst
ohenholz
Pomellen
Nadrensee
11
E28
13
Siadło Dolne
Oder
Kamieniec
Rosow
Schwarzer Tanger
Odra Wschodnia
People
Devices
Items
Me

CONNECTED

Keep Pointing at Satellite to Send Location

Sending location...

**My Location**

| | |
|---|---|
| Location | 53,33810° N, 14,43942° E |
| From | This iPhone |
| Share My Location | ● |

**My Location via Satellite**

| | |
|---|---|
| Last Sent | In Progress |

Sending Location...

**Notifications**

| | |
|---|---|
| Allow Friend Requests | ● |

CONNECTED

Keep Pointing at Satellite to Send Location

Sending location...

My Location

Location 53,33810° N, 14,43942° E

From This iPhone

Share My Location

My Location via Satellite

Last Sent In Progress

Sending Location...

Notifications

Allow Friend Requests

Hohenholzer Forst
ohenholz
Pomellen
Nadrensee
11
E28
13
Siadło Dolne
Oder
Kamieniec
Rosow
Schwarzer Tanger
Odra Wschodnia
People
Devices
Items
Me

Hohenholzer
oh
Siadło
Dolne
Oder
Odra Wschodnia

qmi_satellite_poland.pcapng

qmi.service_id == 0xea

```
No.     Time          Protocol  Length  Info
2899    593.593753    QMI           25  sft Response: Send File
2900    593.593753    QMI          302  sft Request: Send File
2901    593.593757    QMI           20  sft Response: Send File
2902    593.593757    QMI           22  sft Indication: File Transfer Status
2903    593.593758    QMI          555  sft Request: Activation
2904    593.593762    QMI           21  sft Indication: Service Info
2905    593.593769    QMI           20  sft Response: Activation
2941    597.597724    QMI           25  sft Indication: Service Info
2954    600.600671    QMI           28  sft Request: Update Orientation
2955    600.600680    QMI           20  sft Response: Update Orientation
2956    601.600775    QMI           25  sft Indication: Service Info
```

```
> Frame 2903: 555 bytes on wire (4440 bits), 555 bytes captu
  DLT: 147, Payload: qmi (Qualcomm MSM Interface)
v Qualcomm MSM Interface
  > QMUX Header
  > Transaction Header
  > Message Header
  > TLV 0x01 Service Type
  > TLV 0x02 Protocol Mode
  > TLV 0x03 SPS Environment Type (depens on reason)
  > TLV 0x04 Security Credentials: EPKI (8 bytes) + Shared
  > TLV 0x05 EARFCN
  v TLV 0x06 Location Data (GPS Timestamps and Zone)
      TLV Type: 0x06
      TLV Length: 118
      TLV Value [truncated]: b379fb3cfde02c404761831a47ab4
  > TLV 0x07 Cell Search (?)
  > TLV 0x11 Auto Initiate Registration (?)
  > TLV 0x10 Heat Map Data
```

```
0050  c4 00 04 00 c6 00 04 00  c8 00 04 00 ca 00 04 00   ········ ········
0060  cc 00 04 00 01 1a 00 04  00 06 76 00 b3 79 fb 3c   ········ ··v··y·<
0070  fd e0 2c 40 47 61 83 1a  47 ab 4a 40 00 00 76 3b   ··,@Ga·· G·J@··v;
0080  c6 2c 42 40 ff cb b2 6c  c7 f6 12 40 21 3e b2 62   ·,B@···l ···@!>·b
0090  e7 f2 0a 40 76 3b 19 00  00 00 00 00 5f 73 a5 3e   ···@v;·· ····_s·>
00a0  cd cc cc 3d c5 f5 e5 ba  3e 74 52 13 00 00 7a 44   ···=···· >tR···zD
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 03 50 4f 4c  12 00 00 00 00 00 00 00   ·····POL ········
00d0  00 00 00 00 00 00 00 00  00 01 3b aa 28 4d 5e 7e   ········ ··;·(M^~
00e0  03 00 07 01 00 01 11 01  00 00 10 3e 01 06 0f 00   ········ ···>····
00f0  00 00 1e 00 00 00 2d 00  00 00 3c 00 00 00 4b 00   ······-· ··<···K·
0100  00 00 5a 00 00 00 18 00  00 00 20 00 00 00 00 00   ··Z····· ·· ·····
0110  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00   ········ ········
0120  00 03 00 00 00 03 00 00  00 00 06 00 00 00 00 00   ········ ········
0130  00 00 00 0f 00 00 00 00  00 00 00 00 10 00 00 00   ········ ········
0140  00 00 00 00 00 11 00 00  00 00 00 00 00 00 13 00   ········ ········
0150  00 00 00 00 00 00 00 14  00 00 00 00 00 00 00 00   ········ ········
0160  16 00 00 00 01 01 00 00  00 02 00 00 00 03 01 00   ········ ········
0170  00 00 04 00 00 00 03 01  00 00 00 05 00 00 00 03   ········ ········
0180  01 00 00 00 09 00 00 00  03 01 00 00 00 0d 00 00   ········ ········
0190  00 03 01 00 00 00 0e 00  00 00 03 01 00 00 00 14   ········ ········
01a0  00 00 00 03 01 00 00 00  15 00 00 00 03 02 00 00   ········ ········
01b0  00 02 00 00 00 03 02 00  00 00 03 00 00 00 03 02   ········ ········
01c0  00 00 00 09 00 00 00 03  02 00 00 00 0c 00 00 00   ········ ········
01d0  03 02 00 00 00 0f 00 00  00 03 02 00 00 00 14 00   ········ ········
01e0  00 00 03 03 00 00 00 05  00 00 00 03 03 00 00 00   ········ ········
01f0  0b 00 00 00 03 03 00 00  00 12 00 00 00 03 04 00   ········ ········
0200  00 00 02 00 00 00 02 04  00 00 00 04 00 00 00 01   ········ ········
0210  04 00 00 00 0a 00 00 00  03 04 00 00 00 0f 00 00   ········ ········
0220  00 00 05 00 00 00 0d 00  00 00 03                  ········ ···
```

Bytes 108-225: TLV Value (qmi.tlv_value)    Packets: 3918 · Displayed: 108 (2.8%)    Profile: Default

CONNECTED
Keep Pointing at Satellite to Send Location
Sending location...

My Location

| | |
|---|---|
| Location | 53,33810° N, 14,43942° E |
| From | This iPhone |
| Share My Location | ● |

My Location via Satellite

| | |
|---|---|
| Last Sent | In Progress |

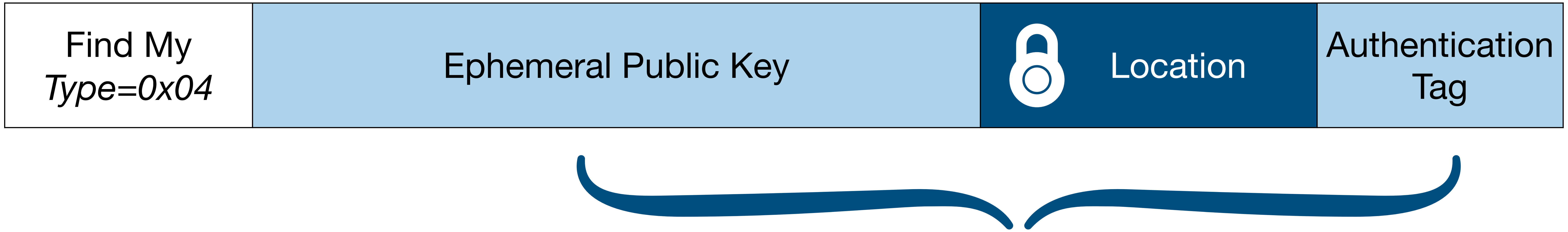
Sending Location...

Notifications

Allow Friend Requests ●

# Sending Custom Messages over Satellite

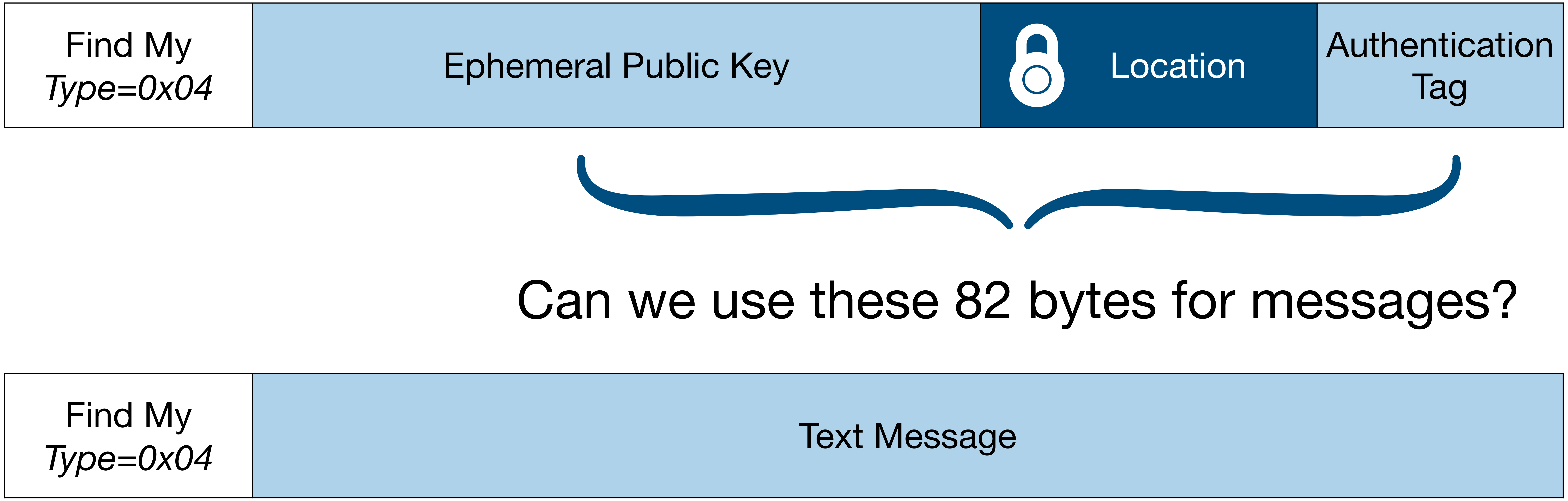
## Reproducing Send My for Apple’s Satellite Communication



Can we use these 82 bytes for messages?

# Sending Custom Messages over Satellite

## Reproducing Send My for Apple’s Satellite Communication



Find My *Type=0x04*

Ephemeral Public Key

🔒 Location

Authentication Tag

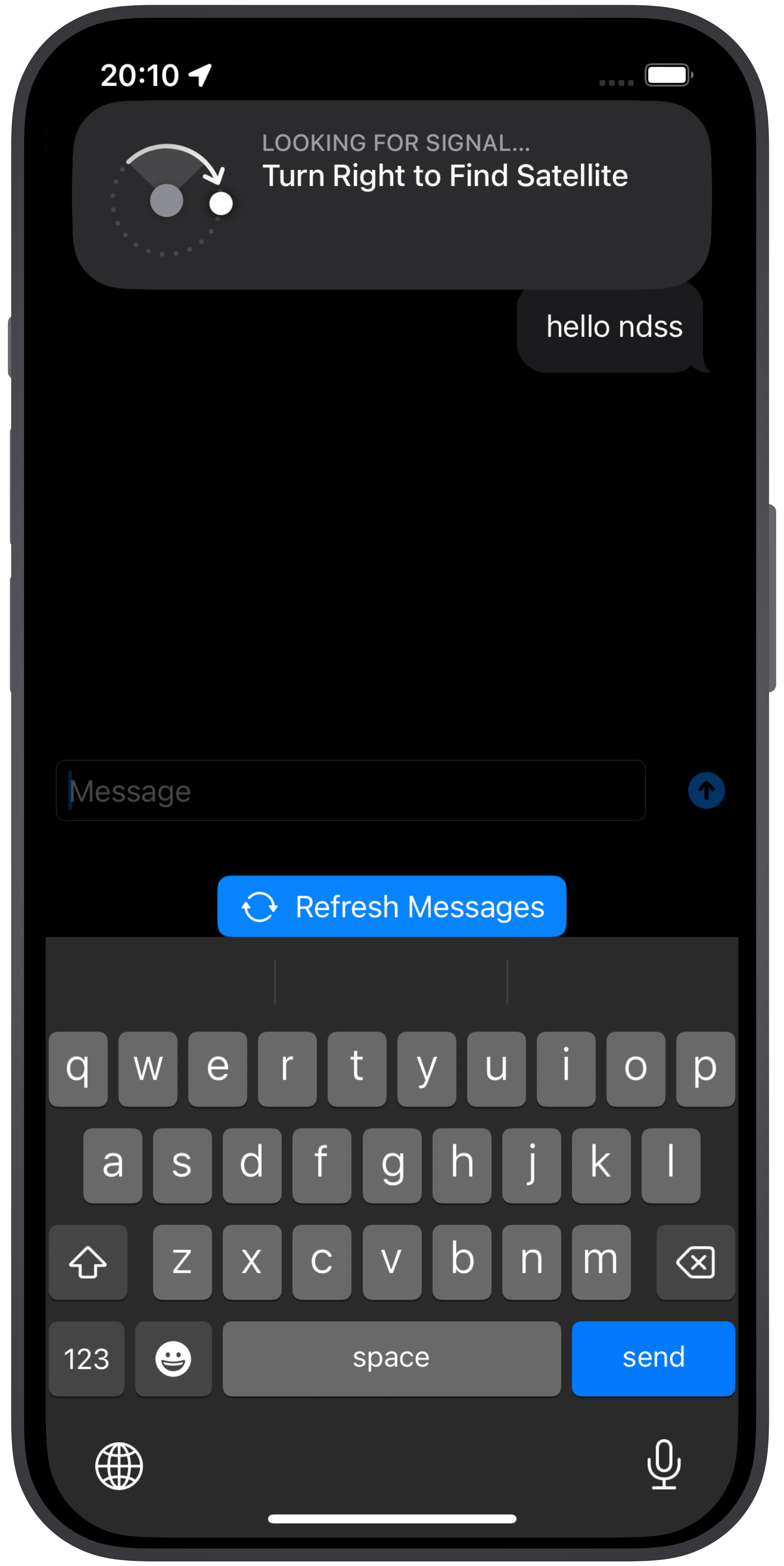
Can we use these 82 bytes for messages?

Find My *Type=0x04*

Text Message

# Sending Satellite Messages

## With Jailbroken iPhones

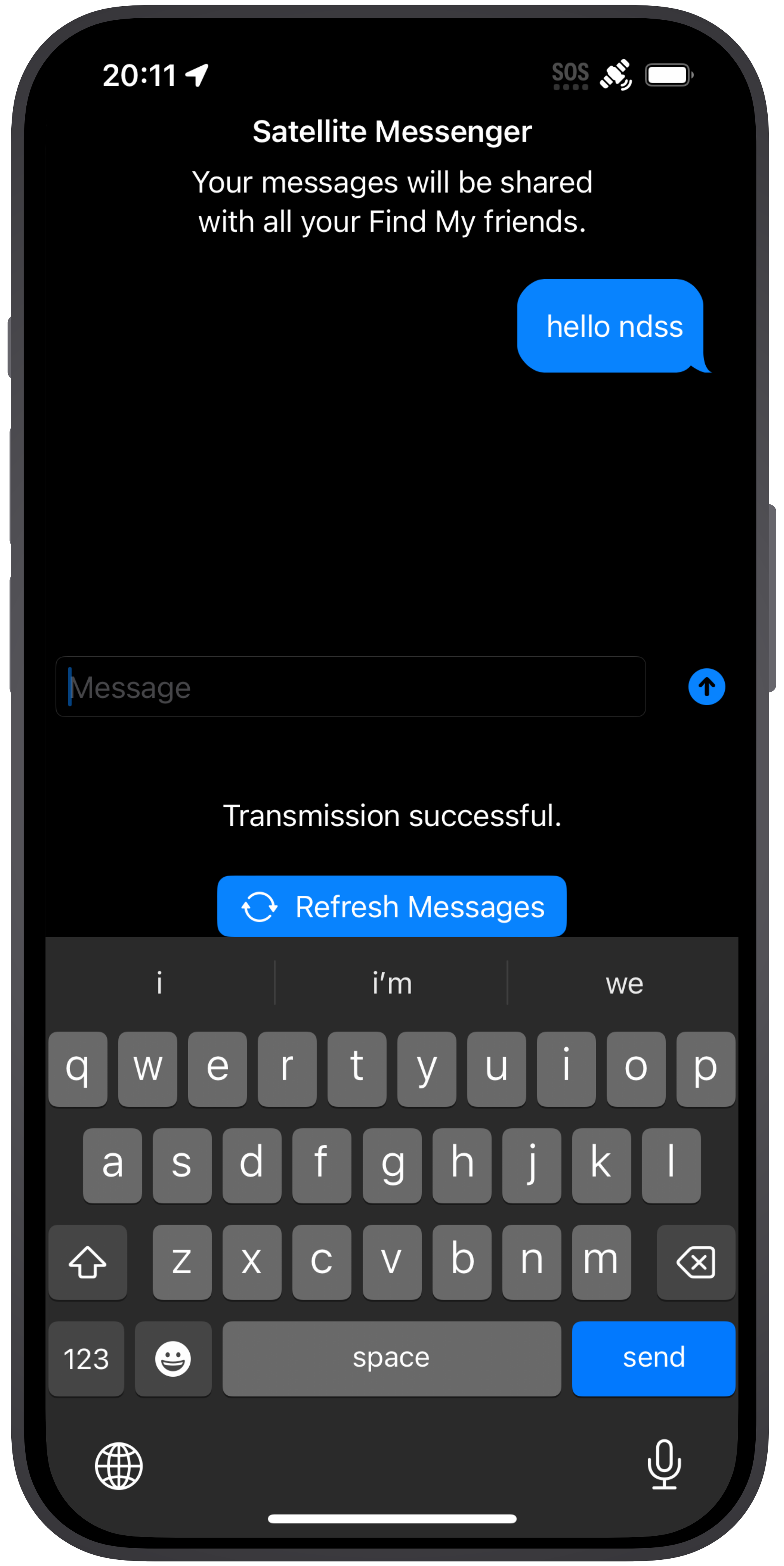

20:10

LOOKING FOR SIGNAL...

Turn Right to Find Satellite

hello ndss

Message


20:11

Satellite Messenger

Your messages will be shared with all your Find My friends.

hello ndss

Message

Transmission successful.

# Available on GitHub

github.com/seemoo-lab/satellite-messenger

# There’s more

## … in our paper

Artifact Evaluated NDSS

Available

Functional

Reproduced

# Starshields for iOS: Navigating the Security Cosmos in Satellite Communication

Jiska Classen*
Hasso Plattner Institute
University of Potsdam
jiska.classen@hpi.de

Alexander Heinrich*
Secure Mobile Networking Lab
TU Darmstadt
aheinrich@seemoo.de

Fabian Portner
Secure Mobile Networking Lab
TU Darmstadt
fportner@seemoo.de

Felix Rohrbach
Cryptoplexity
TU Darmstadt
felix.rohrbach@tu-darmstadt.de

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt
mhollick@seemoo.de

***Abstract*—Apple has integrated satellite communication into their latest iPhones, enabling emergency communication, roadside assistance, location sharing with friends, iMessage, and SMS. This technology allows communication when other wireless services are unavailable. However, the use of satellites poses restrictions on bandwidth and delay, making it difficult to use modern communication protocols with their security and privacy guarantees. To overcome these challenges, Apple designed and implemented a proprietary satellite communication protocol. We are the first to successfully reverse-engineer this protocol and analyze its security and privacy properties. In addition, we develop a simulation-based testbed for testing emergency services without causing emergency calls. Our tests reveal protocol and infrastructure design issues. For example, compact protocol messages come at the cost of missing integrity protection and require an internet-based setup phase. We further demonstrate various restriction bypasses, such as misusing location sharing to send arbitrary text messages on old iOS versions and sending iMessages over satellite from region-locked countries. These bypasses allow us to overcome censorship and operator control of text messaging services.**

### I. Introduction

Apple introduced satellite communication support with the iPhone 14 [5], allowing users to request assistance during emergencies in areas without cellular coverage. Further features include sharing the current location with friends over Find My [10] and requesting roadside assistance [9]. iMessage and SMS text messaging were added in iOS 18 [14].

Apple relies on the satellite network provided by Globalstar, a company operating satellites in Low Earth Orbits (LEOs) at around 1 414 km height, orbiting the earth multiple times a day. We found that the oldest satellite used by Apple was launched in 2007, the same year the first iPhone was released [51]. Operating a 17-year-old infrastructure implicates technological challenges by itself [84], but Apple must also deal with satellites’ fast movement during transmission, high delays, and generally low bandwidth requirements. At the same time, users need to be able to operate satellite communication intuitively under high stress in emergencies. This fact necessitates fast transmissions, ideally within a minute, and high satellite network availability. Apple’s emergency SOS via satellite proved instrumental in saving lives during wildfires and hurricanes, when cellular network communication was no longer possible [52], [81].

Globalstar offers satellite network subscriptions directly to customers for location, text, data, and voice services [34]. In 2015, researchers revealed severe vulnerabilities in Globalstar’s satellite communication protocol and released tools for decoding it [55]. We confirm that these attacks still work as of 2024 to intercept Globalstar’s services. With this troubled security history, Apple invented a novel, proprietary protocol and only shares the Globalstar infrastructure. Apple’s satellite protocol aims to protect highly privacy-sensitive data: A location shared via satellite should only be accessible to the designated recipients. More sensitive data leaves the phone during Emergency SOS via satellite: Health information from the user’s medical ID [15], text messages, location information, and accurate information about the current emergency.

This work represents the first comprehensive investigation into Apple’s satellite services’ security and privacy. We reverse-engineer previously undocumented internals to answer the following research questions: ***RQ1:*** *How are security and privacy features implemented in this resource-constrained satellite communication environment?* ***RQ2:*** *Can users bypass service restrictions imposed by Apple?*

**Contributions.** At the time of writing, only limited related work on the security of end-device to satellite communication exists [55], [46], [84], [86]. We are the first to analyze satellite communication implemented in the iPhone. Our main contributions are:

[*] Both authors contributed equally to this research.

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.240124
www.ndss-symposium.org

- Satellite Protocol Definition
- Reverse Engineering Methodology
- More Bypasses and leaks
- How to design secure satellite communication?

@Sn0wfreeze

@naehrdine

jiskac