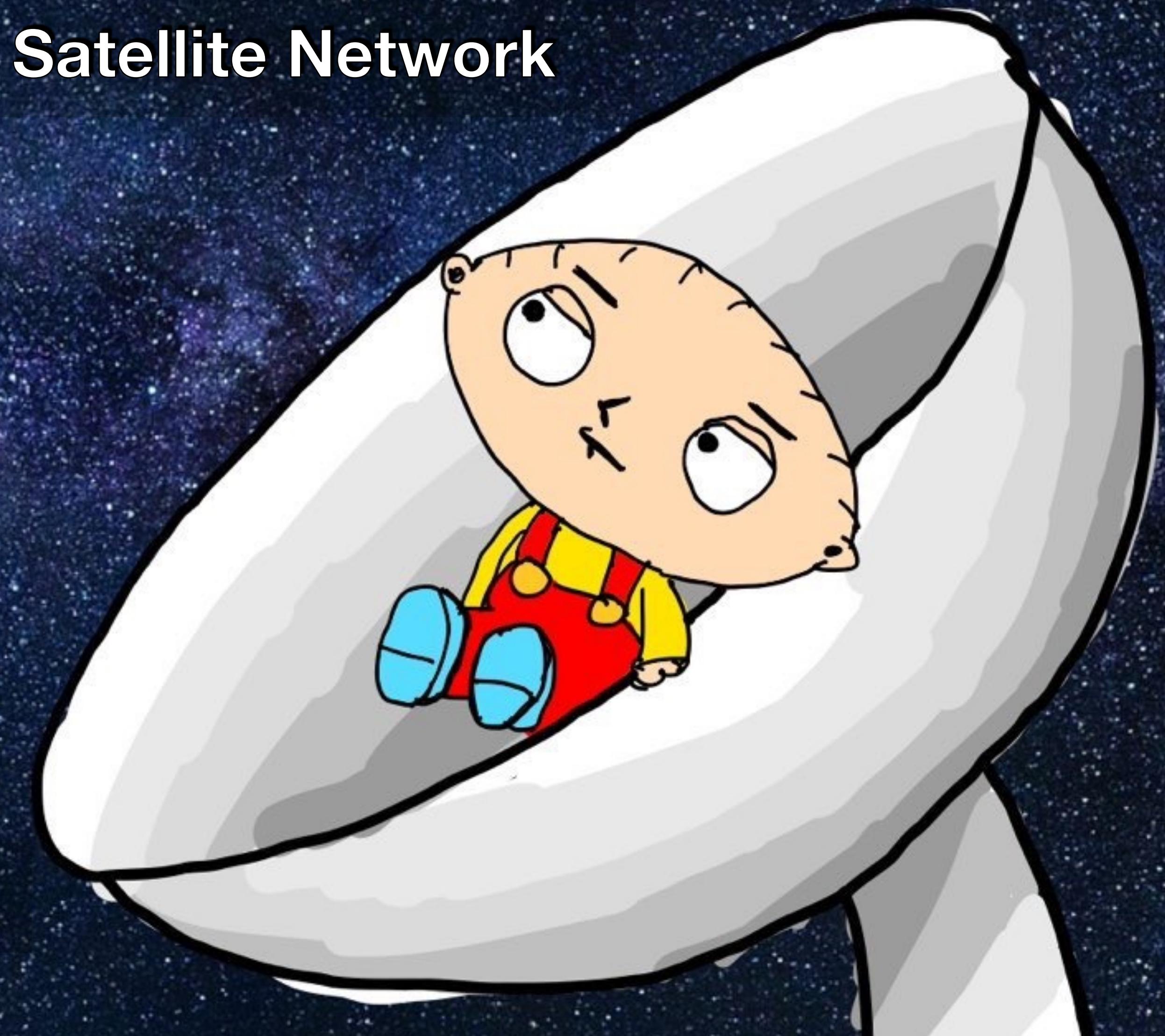


Lois... Ma... Mommy...

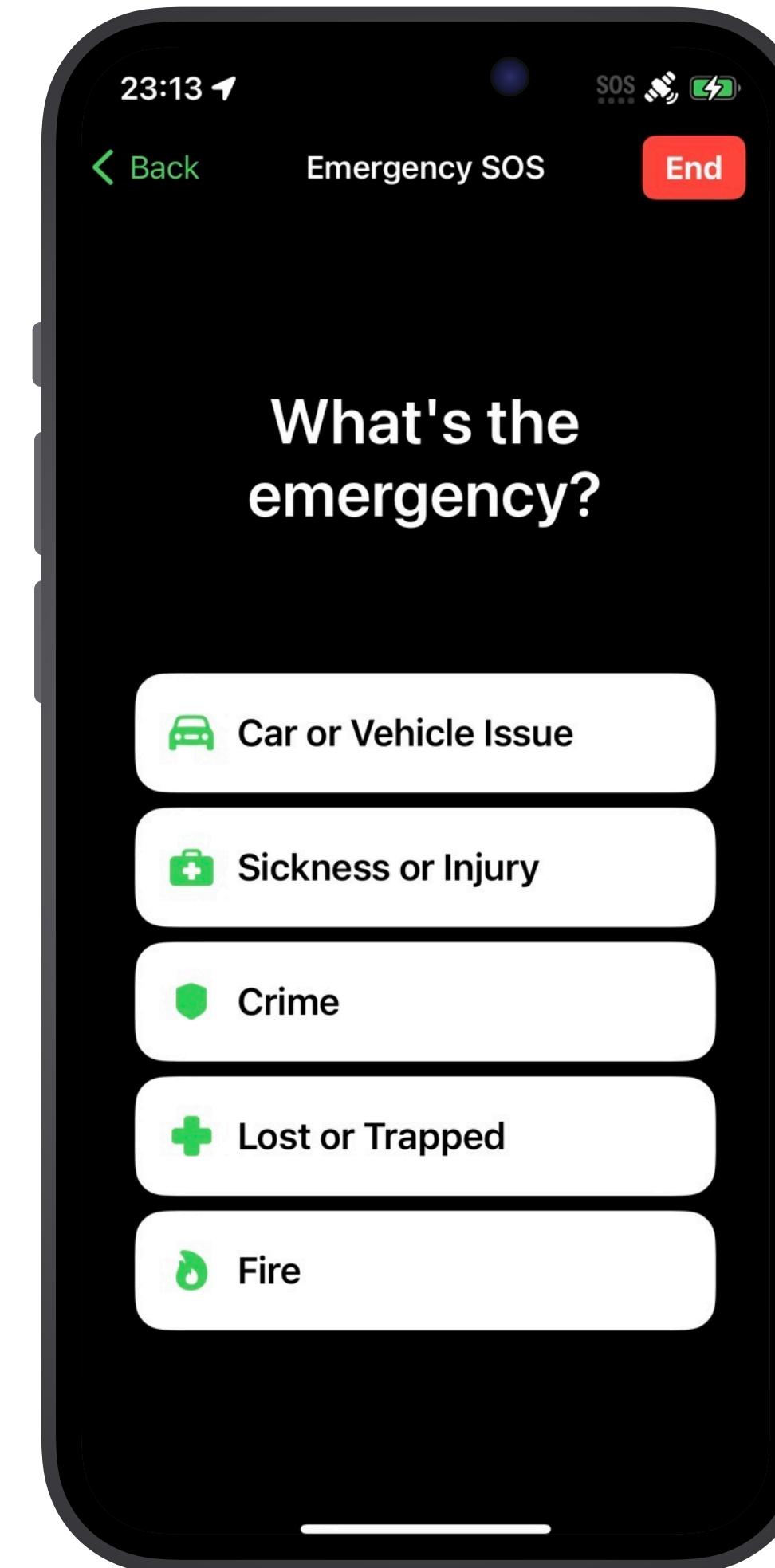
Stewie Talking to Apple's Satellite Network



Alexander Heinrich & Jiska Classen



Emergency SOS



Requirements

- No Wi-Fi or cellular coverage
- Failed emergency call
- SOS button appears in phone menu



Find My Over Satellite



Requirements

- No Wi-Fi or cellular coverage
- SIM installed
- Friends added while online

Demo Mode



Requirements

- Satellite service available on the specific iPhone

Internally called "Emergency Try Out"

Availability



iOS 16.1



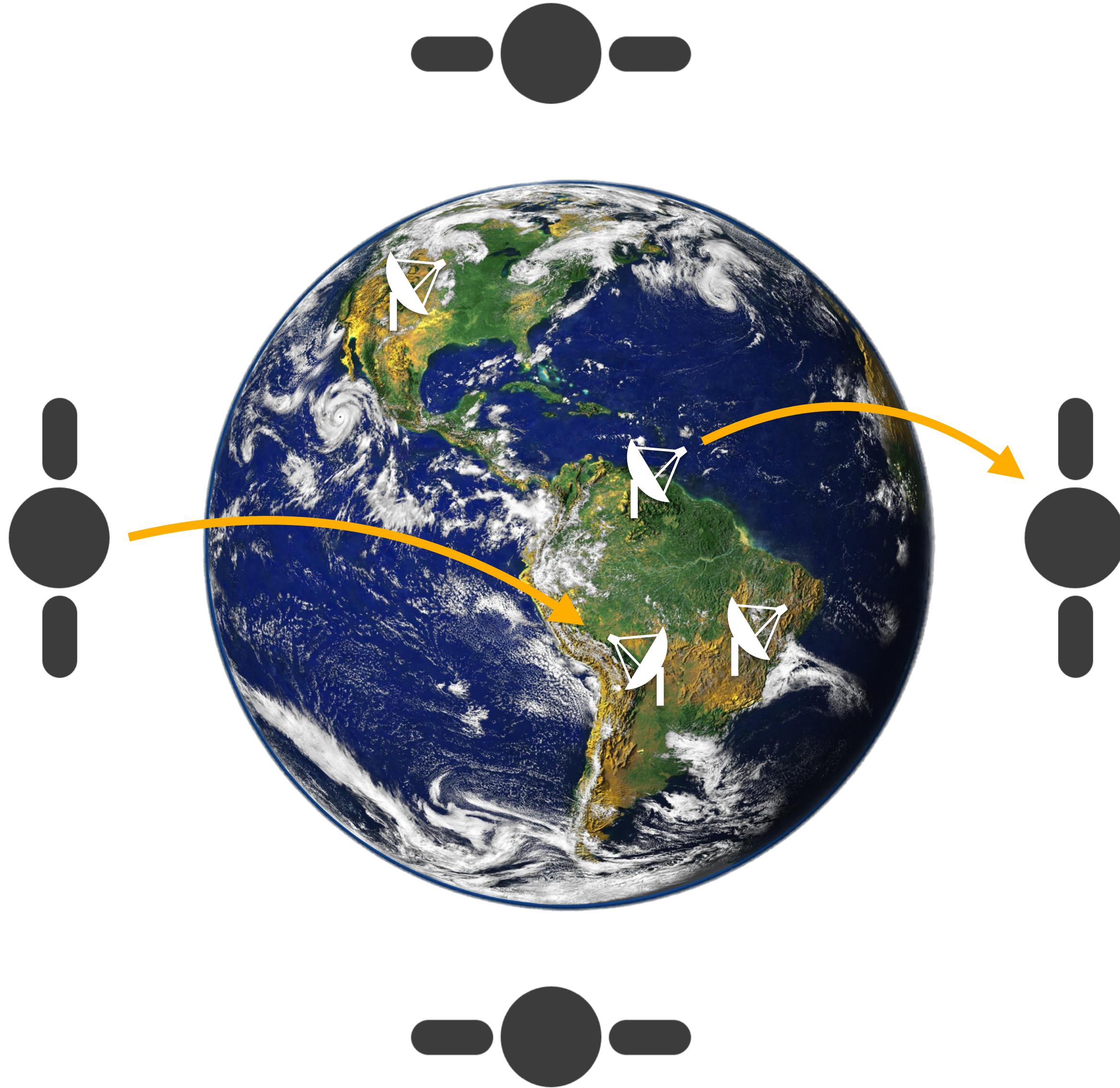
iOS 16.2



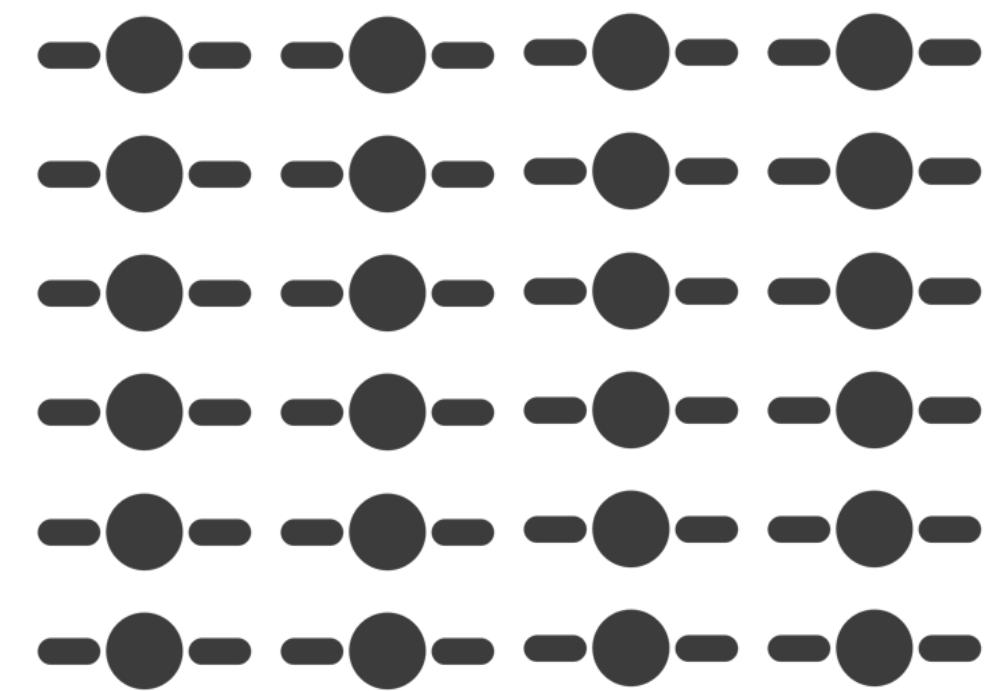
iOS 16.4

Globalstar Satellite Network





Stats



Minimum 28 Satellites

1400 km (870 miles) altitude



24 ground stations

Closest one in France

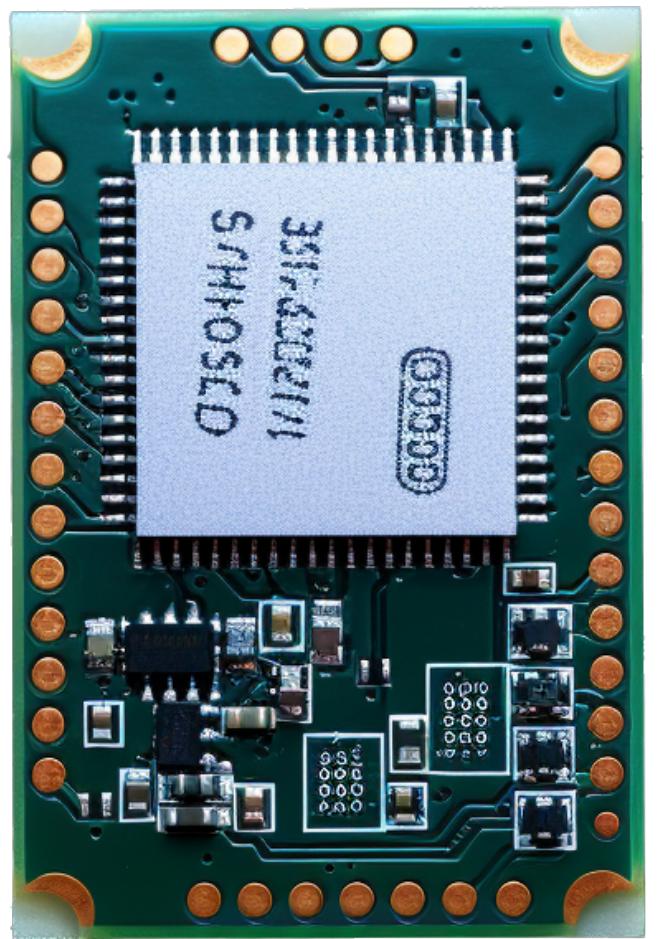
Provided Services



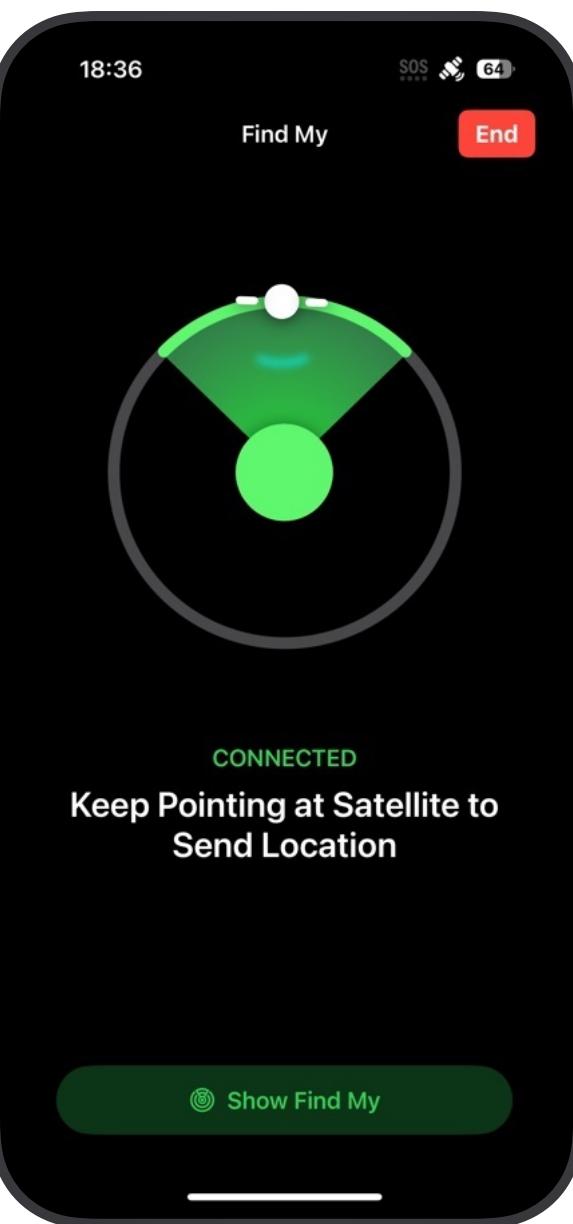
Phones



Messengers

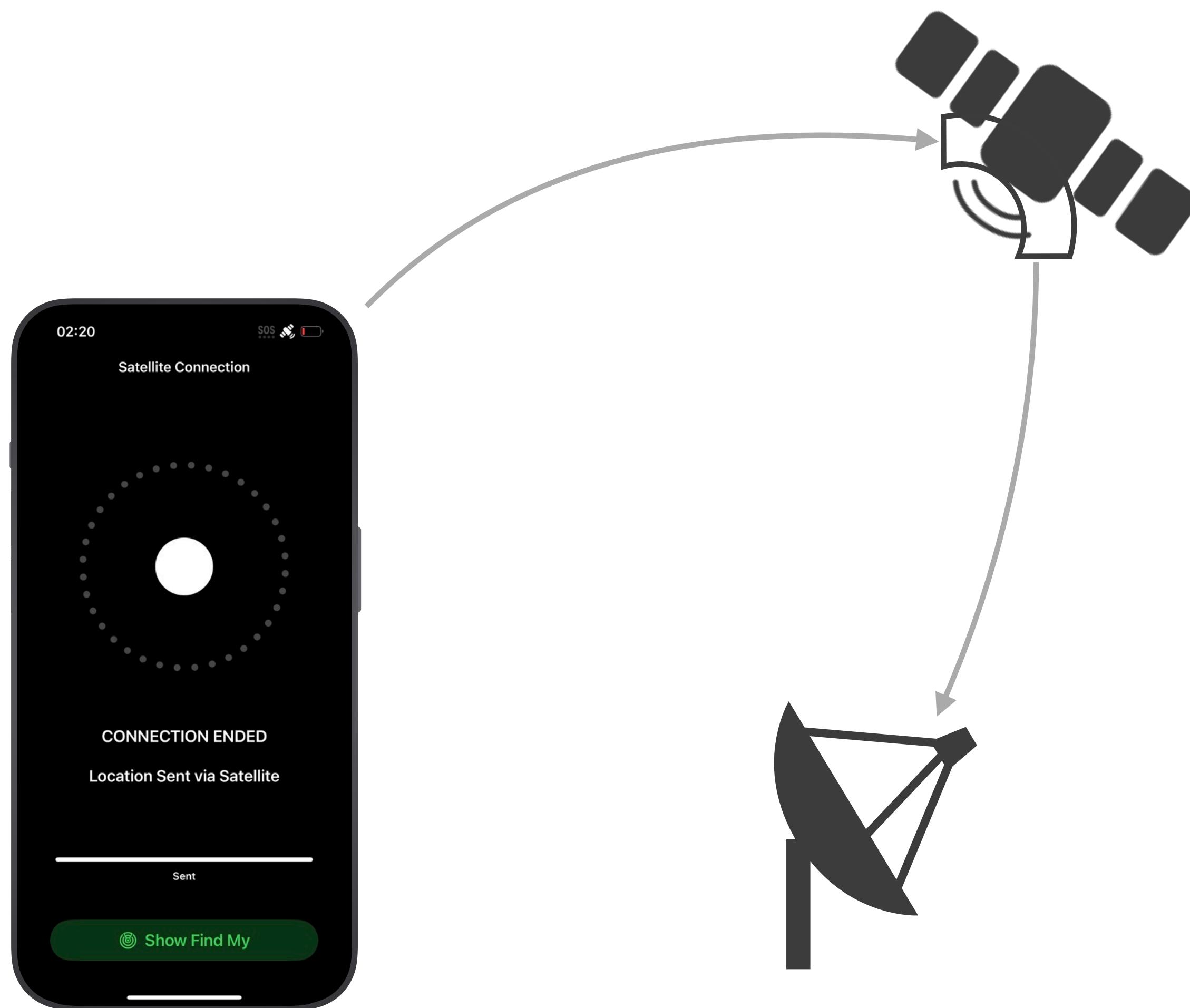


IoT Chips



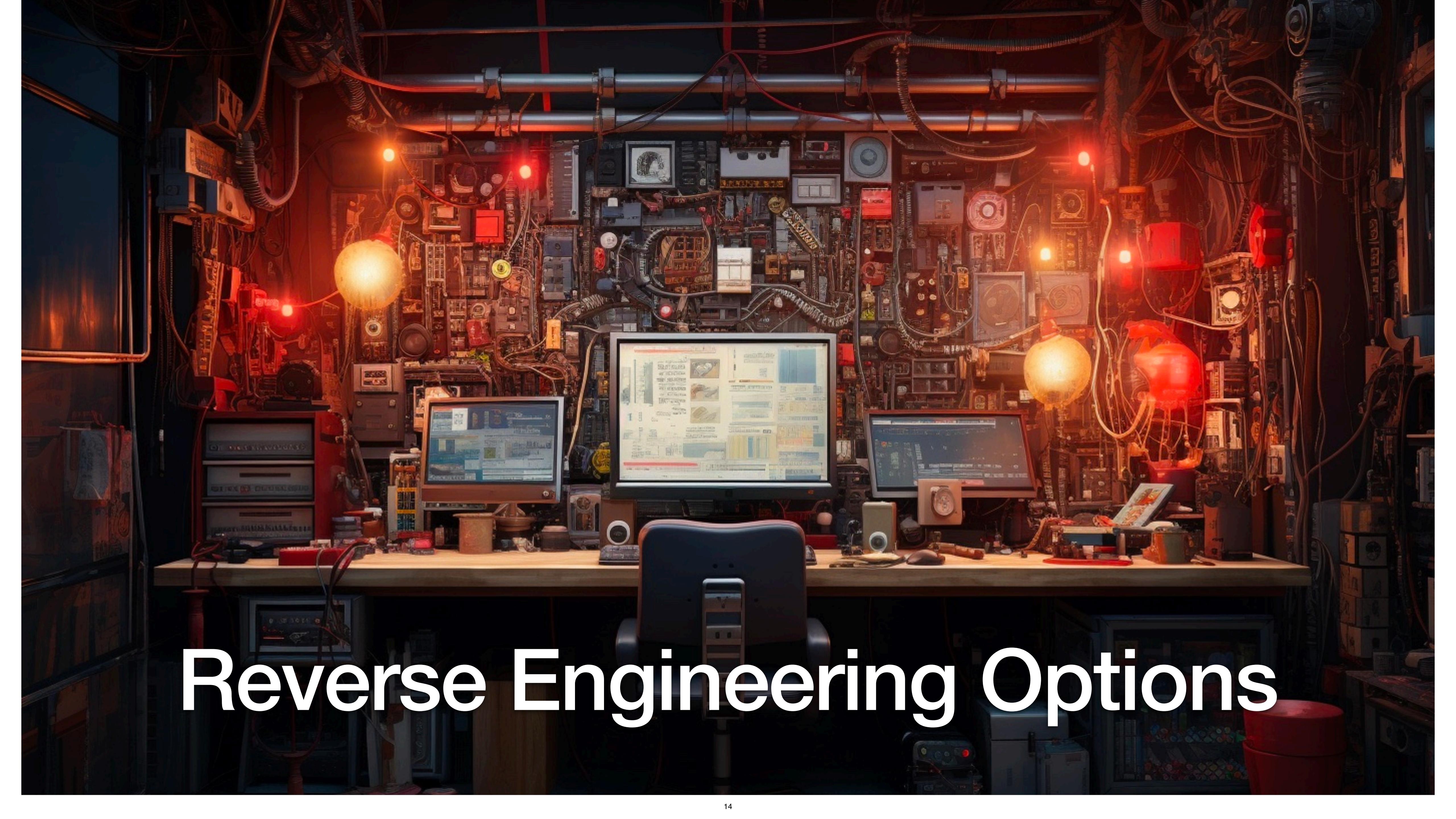
iPhones

Satellite Communication Basis



- Bent-pipe satellites
- Messages are reflected
- Decoding at the ground station
- Maximum 9600bps





Reverse Engineering Options

ios 16 jelbrek for iphone 14, wen eta?



Static reversing & staring on iPhone 14 logs...

The screenshot shows a web browser window for developer.apple.com. The top navigation bar includes links for Apple Developer, News, Discover, Design, Develop, Distribute, Support, Account, and a search icon. Below this, a secondary navigation bar for 'Bug Reporting' features links for Overview, Profiles and Logs, and Feedback Assistant, with 'Feedback Assistant' being the active tab. The main content area is titled 'Profiles and Logs' and contains a descriptive paragraph about how profiles and logs help developers provide information to Apple for bug investigation. Below this, a filter bar allows users to select from All, iOS, macOS, tvOS, watchOS, Other, or baseband. The 'baseband' option is selected and highlighted with a blue border. Two items are listed under the 'baseband' category: 'Baseband for iOS' and 'Baseband for watchOS', each with a 'Instructions' and 'Profile' link.

Profiles and Logs

These profiles and logs are for developers to use in order to provide information about bugs to Apple. Get details on providing logs, reproducible test cases, and other information that will help us investigate and diagnose reported issues.

All iOS macOS tvOS watchOS Other **baseband**

Baseband for iOS [Instructions](#) [Profile](#)

Baseband for watchOS [Instructions](#) [Profile](#)

system_logs.logarchive				7,395 messages	ANY	qmux			
Type	Date & Time	Process	Message	Reveal	Activities	Clear	Reload	Info	Share
	2023-03-30 16:24:46.286962+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 3F 00 00 A0 09 04 01 06 04 0C 00 10 00 1E 00 83 6B 70 30 05 9F 83 6F 01 05 30 0						
	2023-03-30 16:24:46.287656+0200	CommCenter	QMI: Svc=0xe4(AWD) Ind MsgId=0x1010 Bin=['01 A6 00 80 E4 02 04 7E 0C 10 10 9A 00 52 97 00 00 00 00 64 69 00 00 A0 00 00 00 62 A1 0C 00 62 A						
	2023-03-30 16:24:46.290241+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 3F 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 11 00']						
	2023-03-30 16:24:46.290303+0200	CommCenter	#I qmux: [qmux1] queueing qmux pdu for svc=234 client=1 (txid=64 msgid=0xa000) [tx-slot=1, rx-pending=0]						
	2023-03-30 16:24:46.290311+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 40 00 00 A0 09 04 01 06 04 0C 00 11 00 1E 00 6B 30 05 9F 83 6F 01 6D 30 05 9F 8						
	2023-03-30 16:24:46.293508+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 40 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 12 00']						
	2023-03-30 16:24:46.293554+0200	CommCenter	#I qmux: [qmux1] queueing qmux pdu for svc=234 client=1 (txid=65 msgid=0xa000) [tx-slot=1, rx-pending=0]						
	2023-03-30 16:24:46.293560+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 41 00 00 A0 09 04 01 06 04 0C 00 12 00 1E 00 60 01 61 BF 83 61 81 8A 9F 83 6A 0						
	2023-03-30 16:24:46.296464+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 41 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 13 00']						
	2023-03-30 16:24:46.296511+0200	CommCenter	#I qmux: [qmux1] queueing qmux pdu for svc=234 client=1 (txid=66 msgid=0xa000) [tx-slot=1, rx-pending=0]						
	2023-03-30 16:24:46.296519+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 42 00 00 A0 09 04 01 06 04 0C 00 13 00 1E 00 6F 02 00 EB 30 06 9F 83 6F 02 00 E						
	2023-03-30 16:24:46.301315+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 42 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 14 00']						
	2023-03-30 16:24:46.301323+0200	CommCenter	QMI: Svc=0xe4(AWD) Ind MsgId=0x1011 Bin=['01 25 00 80 E4 01 04 77 0C 11 10 19 00 53 16 00 00 00 00 64 69 00 00 A0 00 00 00 62 A1 0C 00 0C 0						
	2023-03-30 16:24:46.301378+0200	CommCenter	#I qmux: [qmux1] queueing qmux pdu for svc=234 client=1 (txid=67 msgid=0xa000) [tx-slot=1, rx-pending=0]						
	2023-03-30 16:24:46.301386+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 43 00 00 A0 09 04 01 06 04 0C 00 14 00 1E 00 84 00 81 D0 30 0C 9F 84 08 02 02 4						
	2023-03-30 16:24:46.301800+0200	CommCenter	QMI: Svc=0xe4(AWD) Ind MsgId=0x1011 Bin=['01 25 00 80 E4 02 04 7F 0C 11 10 19 00 53 16 00 00 00 00 64 69 00 00 A0 00 00 00 62 A1 0C 00 0C 0						
	2023-03-30 16:24:46.304205+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 43 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 15 00']						
	2023-03-30 16:24:46.304286+0200	CommCenter	#I qmux: [qmux1] queueing qmux pdu for svc=234 client=1 (txid=68 msgid=0xa000) [tx-slot=1, rx-pending=0]						
	2023-03-30 16:24:46.304296+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 44 00 00 A0 09 04 01 06 04 0C 00 15 00 1E 00 03 45 9F 84 09 02 03 DB 30 0C 9F 8						
	2023-03-30 16:24:46.308140+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 44 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 16 00']						
	2023-03-30 16:24:46.308196+0200	CommCenter	#I qmux: [qmux1] queueing qmux pdu for svc=234 client=1 (txid=69 msgid=0xa000) [tx-slot=1, rx-pending=0]						
	2023-03-30 16:24:46.308203+0200	CommCenter	QMI: Svc=0xea(SFT) Req MsgId=0xa000 Bin=['01 15 04 00 EA 01 00 45 00 00 A0 09 04 01 06 04 0C 00 16 00 1E 00 02 7F 30 0C 9F 84 08 02 02 5B 9F 8						
	2023-03-30 16:24:46.311379+0200	CommCenter	QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 45 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 17 00']						

Showing: Last 5 Minutes

CommCenter (libATCommandStudioDynamic.dylib)

Subsystem: com.apple.telephony.bb Category: qmux [Hide](#)

Activity ID: 0 Thread ID: 0xe101 PID: 95

Volatile

2023-03-30 16:24:46.301315+0200

QMI: Svc=0xea(SFT) Resp MsgId=0xa000 Bin=['01 18 00 80 EA 01 02 42 00 00 A0 0C 00 02 04 00 00 00 00 40 02 00 14 00']

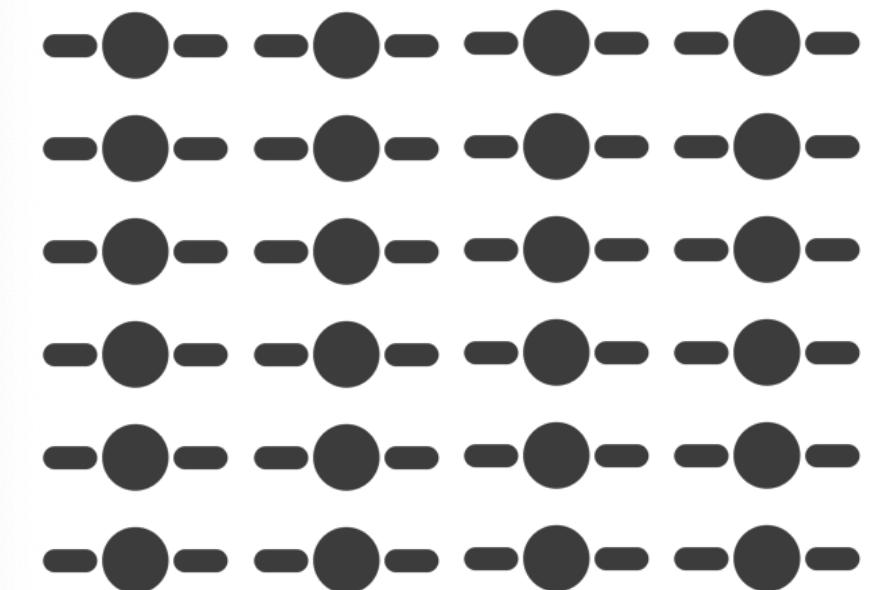
Send current device orientation to modem, and then send satellite positions, one file per active satellite.

No.	Time	Protocol	Length	Info
10541	01:08:06.486985	QMI	28	sft Request: Update Orientation
10542	01:08:06.486994	QMI	20	sft Response: Update Orientation
10818	01:08:09.489917	QMI	4056	sft Request: S4 Config Segement
10821	01:08:09.489923	QMI	20	sft Response: S4 Config Segement
10822	01:08:09.489923	QMI	1046	sft Request: Send File
10829	01:08:09.489929	QMI	25	sft Response: Send File
10830	01:08:09.489929	QMI	1046	sft Request: Send File
10836	01:08:09.489936	QMI	25	sft Response: Send File
10837	01:08:09.489936	QMI	1046	sft Request: Send File
10839	01:08:09.489941	QMI	25	sft Response: Send File
10840	01:08:09.489941	QMI	1046	sft Request: Send File
10843	01:08:09.489946	QMI	25	sft Response: Send File
10844	01:08:09.489946	QMI	1046	sft Request: Send File
10845	01:08:09.489950	QMI	25	sft Response: Send File
10846	01:08:09.489950	QMI	1046	sft Request: Send File
10847	01:08:09.489953	QMI	25	sft Response: Send File
10848	01:08:09.489953	QMI	1046	sft Request: Send File
10849	01:08:09.489957	QMI	25	sft Response: Send File
10850	01:08:09.489957	QMI	1046	sft Request: Send File
10853	01:08:09.489961	QMI	25	sft Response: Send File
10854	01:08:09.489961	QMI	1046	sft Request: Send File
10855	01:08:09.489964	QMI	25	sft Response: Send File
10856	01:08:09.489964	QMI	1046	sft Request: Send File
10857	01:08:09.489967	QMI	25	sft Response: Send File
10858	01:08:09.489967	QMI	1046	sft Request: Send File
10859	01:08:09.489970	QMI	25	sft Response: Send File

> Frame 10541: 28 bytes on wire (224 bits), 28 bytes captured (224 bits) on interface -, id 0
 DLT: 147, Payload: qmi (Qualcomm MSM Interface)
 ▾ Qualcomm MSM Interface
 ▾ QMUX Header
 T/F: 1

Service Name (qmi.service_name)

Packets: 12176 · Displayed: 108 (0.9%) · Dropped: 0 (0.0%)



Thanks @Lukas Arnold for building Wireshark dissectors for Apple's proprietary QMI services!

Send an encrypted message.
Not present during Try Out mode!

qmi.service_name == "QMI Stewie Service"

No.	Time	Protocol	Length	Info
10908	01:08:10.490043	QMI	22	sft Indication: File Transfer Status
10909	01:08:10.490043	QMI	578	sft Request: Activation
10910	01:08:10.490049	QMI	21	sft Indication: Service Info
10915	01:08:10.490075	QMI	20	sft Response: Activation
10988	01:08:14.494518	QMI	25	sft Indication: Service Info
10989	01:08:14.494549	QMI	28	sft Request: Update Orientation
10990	01:08:14.494554	QMI	20	sft Response: Update Orientation
11013	01:08:17.497726	QMI	25	sft Indication: Service Info
11014	01:08:17.497726	QMI	36	sft Indication: Service Info
11015	01:08:17.497727	QMI	13	sft Request: Initiate Registration
11016	01:08:17.497733	QMI	20	sft Response: Initiate Registration
11033	01:08:20.500286	QMI	36	sft Indication: Service Info
11034	01:08:20.500286	QMI	32	sft Indication: Service Info
11053	01:08:22.502845	QMI	36	sft Indication: Service Info
11066	01:08:25.505408	QMI	32	sft Indication: Service Info
11067	01:08:25.505408	QMI	25	sft Indication: Service Info
11068	01:08:25.505408	QMI	60	sft Indication: Security Config Usage
11069	01:08:25.505408	QMI	42	sft Indication: Service Info
11070	01:08:25.505411	QMI	118	sft Request: Send Message
11071	01:08:25.505416	QMI	20	sft Response: Send Message
11090	01:08:27.507964	QMT	42	sft Indication: Service Info

TLV 0x01 Message UUID
TLV Type: 0x01
TLV Length: 16
TLV Value: 6b5b514bbf654faabe6dfcbbe3fa44b2

TLV 0x02 Encrypted Contents
TLV Type: 0x02
TLV Length: 83
TLV Value: 0404c7082b3fb901a2080df91548192f8a6212af22449a48f6c5fbb167ebffb89892536c...

0000	01 75 00 00 ea 01 00 50 00 01 13 69 00 01 10 00	.u.....P ..i....
0010	6b 5b 51 4b bf 65 4f aa be 6d fc bb e3 fa 44 b2	k[QK·e0· ·m···D·
0020	02 53 00 04 04 c7 08 2b 3f b9 01 a2 08 0d f9 15	·S···+ ?···

Service Name (qmi.service_name) Packets: 12176 · Displayed: 108 (0.9%) · Dropped: 0 (0.0%) Profile: Default

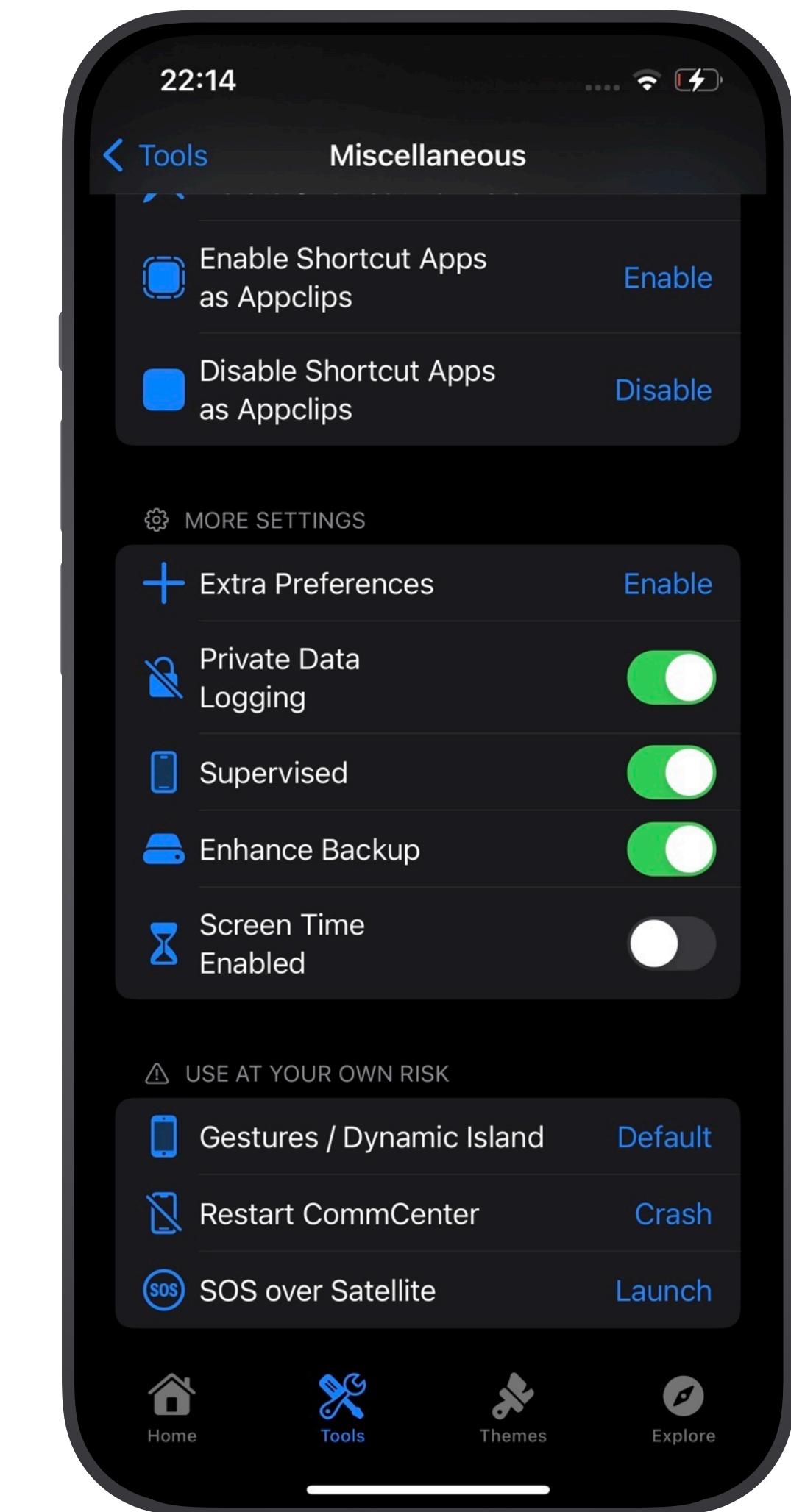
Activation + Security Config, containing Ephemeral Public Encryption Key (EPKI) and further data.
Not present during Try Out mode!

Indicator that the message was sent.

No.	Time	Protocol	Length	Info
11145	01:08:40.520770	QMI	42	SIM INITIALIZATION SERVICE INFO
11159	01:08:40.520772	QMI	42	sft Indication: Service Info
11160	01:08:40.520773	QMI	515	sft Request: GPS Data Update
11162	01:08:40.520776	QMI	20	sft Response: GPS Data Update
11175	01:08:43.523330	QMI	42	sft Indication: Service Info
11182	01:08:44.524578	QMI	28	sft Request: Update Orientation
11183	01:08:44.524585	QMI	20	sft Response: Update Orientation
11194	01:08:45.525484	QMI	28	sft Request: Update Orientation
11195	01:08:45.525492	QMI	20	sft Response: Update Orientation
11198	01:08:45.525894	QMI	42	sft Indication: Service Info
11199	01:08:46.526186	QMI	28	sft Request: Update Orientation
11200	01:08:46.526195	QMI	20	sft Response: Update Orientation
11209	01:08:47.527393	QMI	28	sft Request: Update Orientation
11210	01:08:47.527398	QMI	20	sft Response: Update Orientation
11213	01:08:48.528096	QMI	28	sft Request: Update Orientation
11214	01:08:48.528110	QMI	20	sft Response: Update Orientation
11217	01:08:48.528449	QMI	36	sft Indication: Message TX Status
11218	01:08:48.528449	QMI	42	sft Indication: Service Info
11219	01:08:48.528464	QMI	17	sft Request: Deactivate
11220	01:08:48.528469	QMI	20	sft Response: Deactivate
11223	01:08:49.529079	QMI	24	sft Indication: Deactivation Complete
▼ TLV 0x01 Message UUID				
TLV Type: 0x01				
TLV Length: 16				
TLV Value: 6b5b514bbf654faabe6dfcbbe3fa44b2				
▼ TLV 0x02 Result				
TLV Type: 0x02				
TLV Length: 1				
TLV Value: 00				
0000	01 23 00 80 ea 01 04 34 00 02 13 17 00 01 10 00		.	#.....4
0010	6b 5b 51 4b bf 65 4f aa be 6d fc bb e3 fa 44 b2		k[QK·e0· ·m···D·	
0020	02 01 00 00		

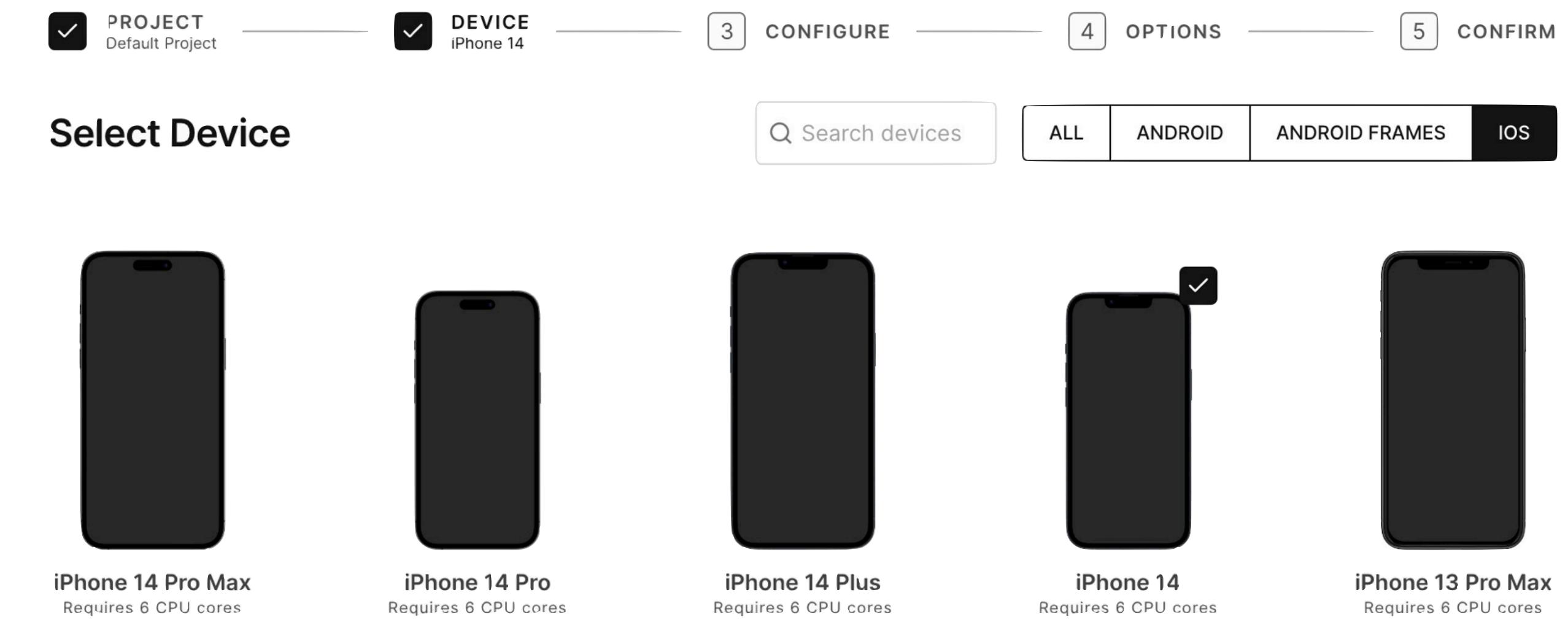
Cowabunga

- Works on iPhone 14 with iOS 16.1.2
- Made some custom tweaks
 - Enhanced logging even when no profile is available
 - Backup more data
 - Crash CommCenter to observe initialisation



Corellium

- Jailbroken iOS 16 on iPhone 14
- Partially thinks it has satellite features
- Easy dynamic instrumentation



Security Research Device

- iPhone 13 mini
- Modem doesn't actually support satellite services
- Most binaries required for satellite services still present
- Can we make it talk to a satellite?

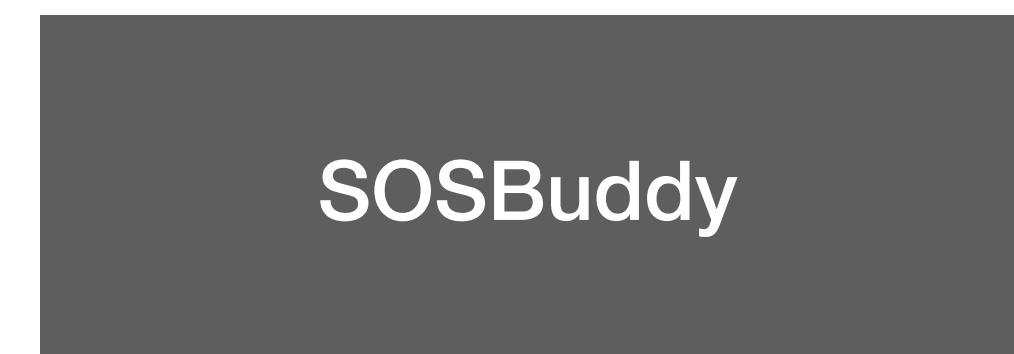
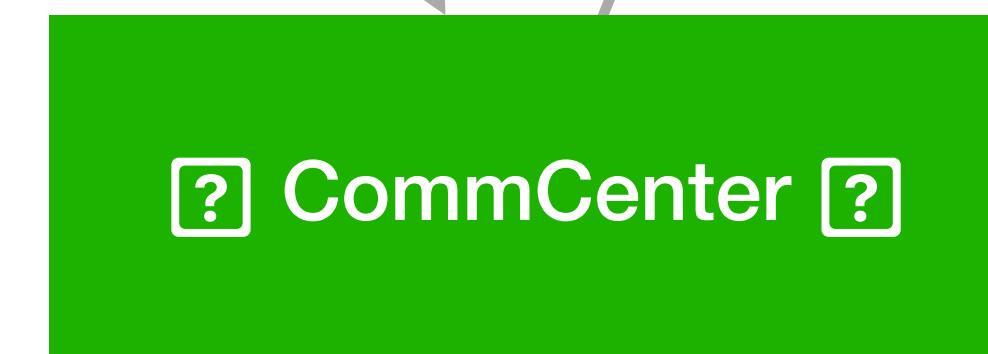
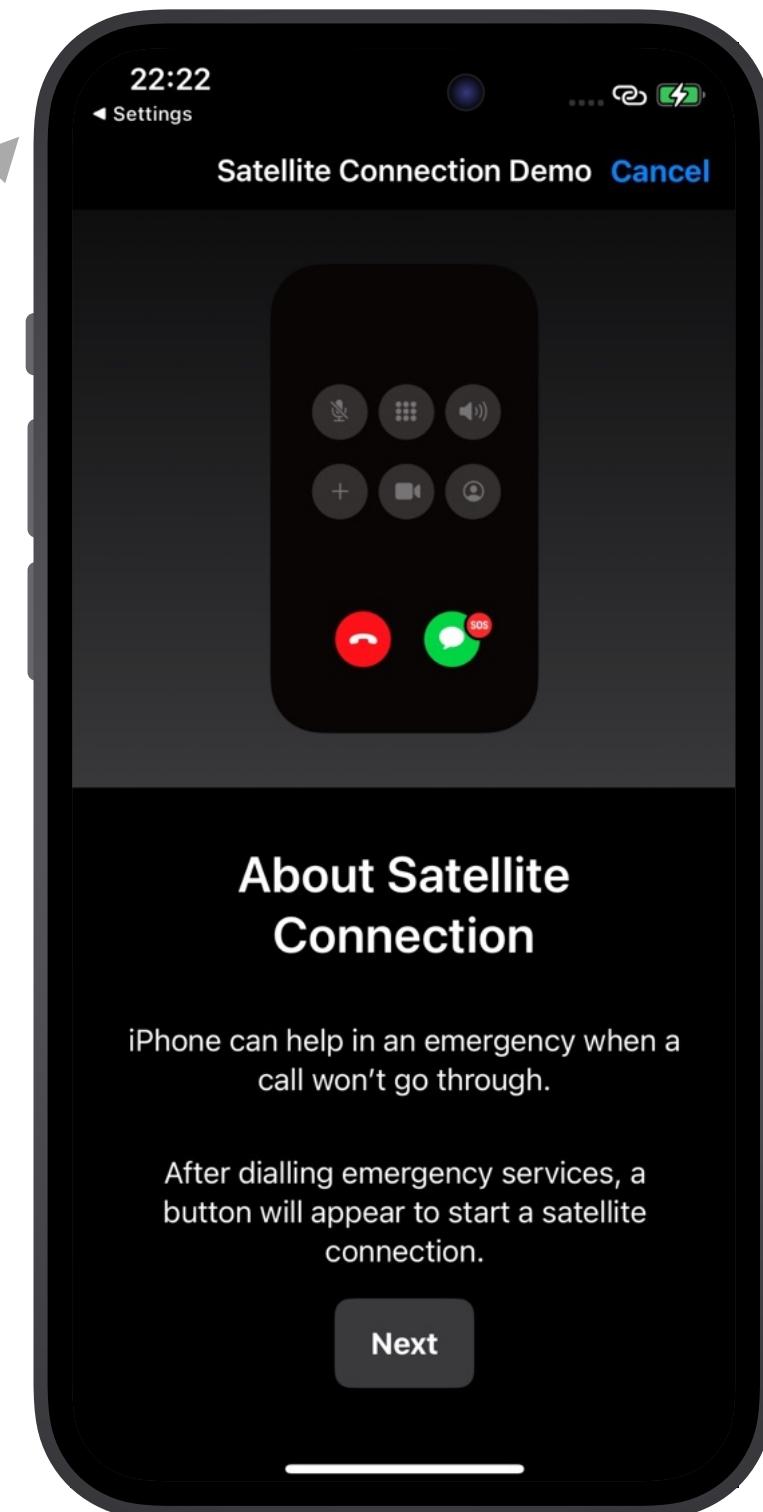


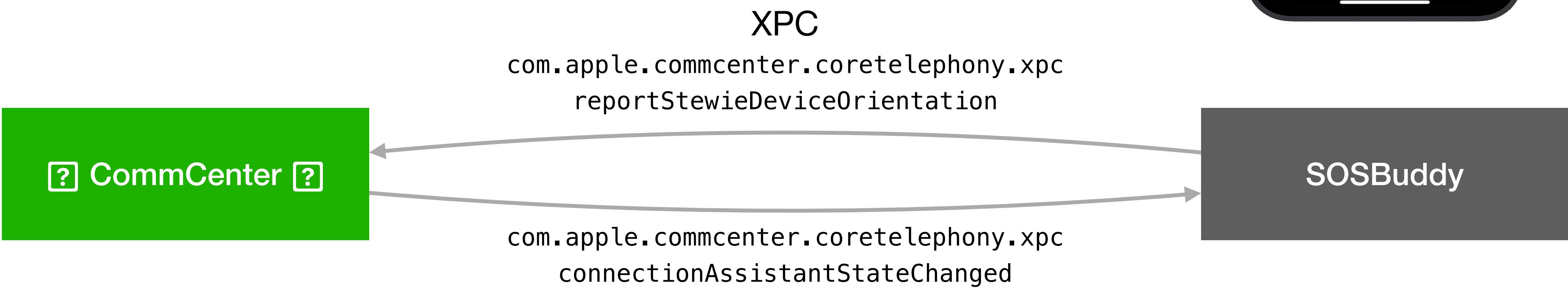
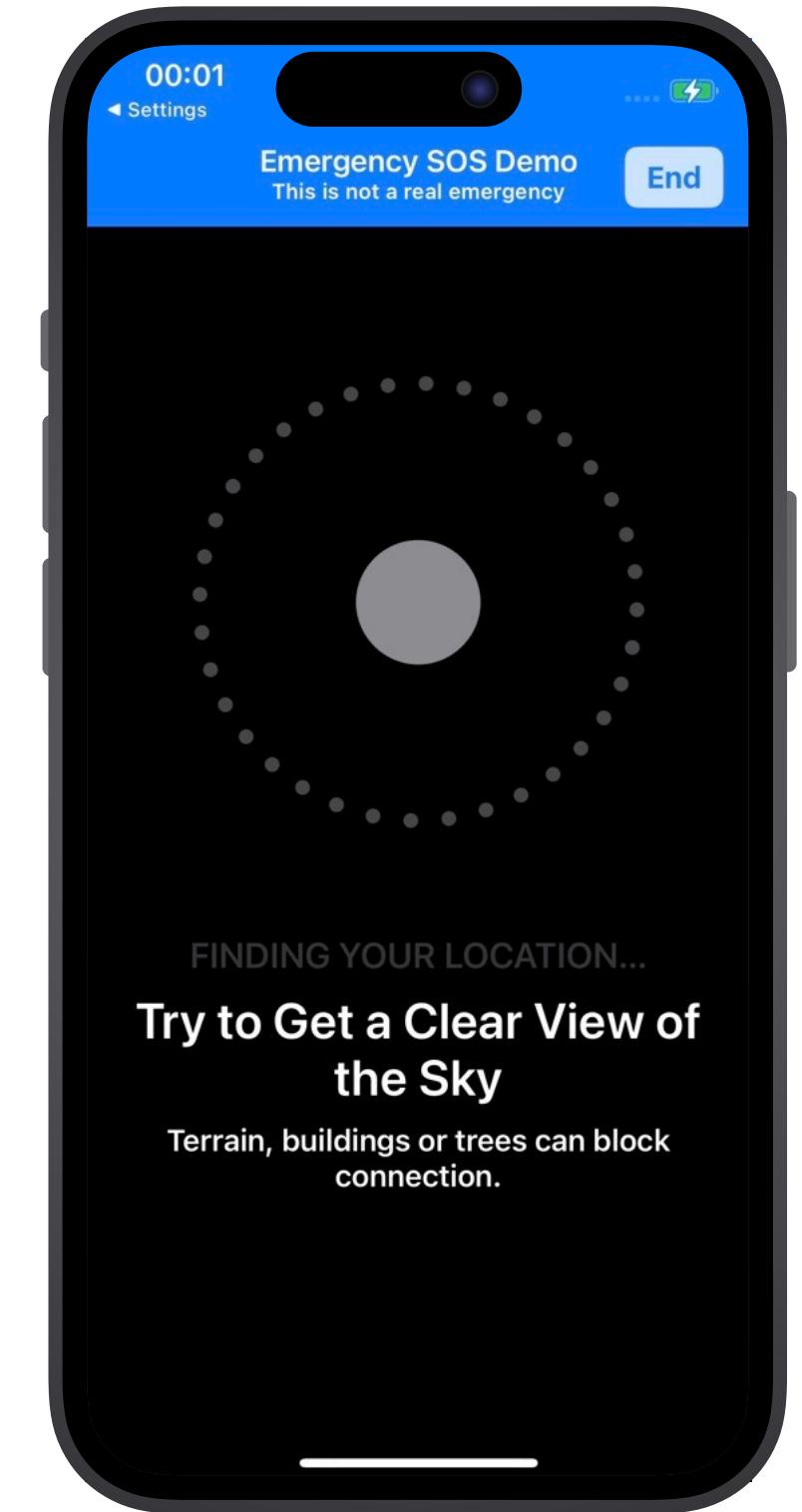
Internal Components

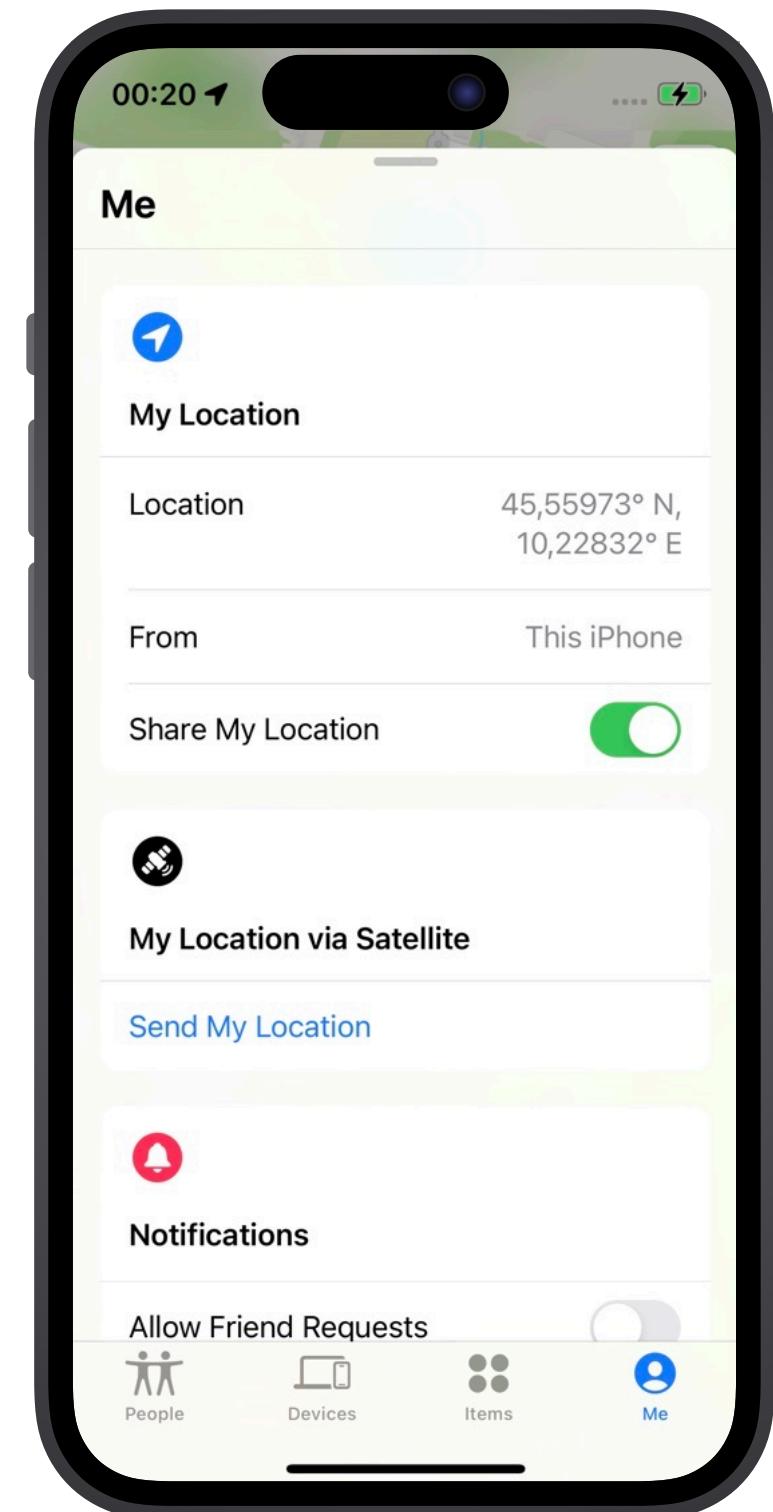


XPC
com.apple.commcenter.coretelephony.xpc
requestStewieWithContext, reason=5
(EmergencyTryOut)

Launch via URL
x-apple-sosbuddy://request?
reason=OfferEmergencyTryOut



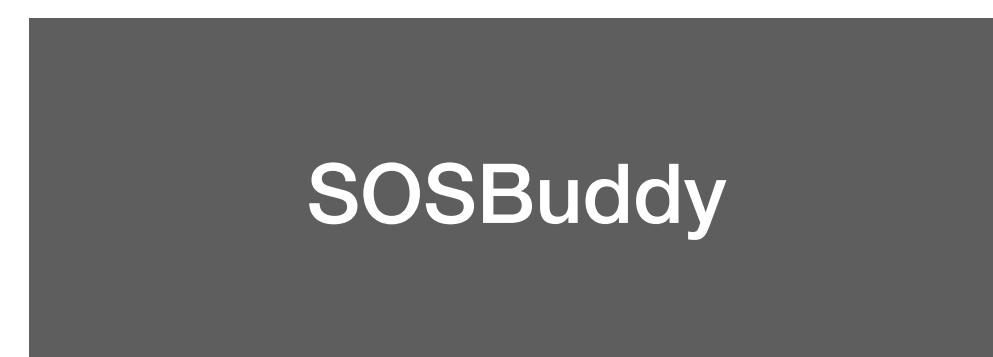
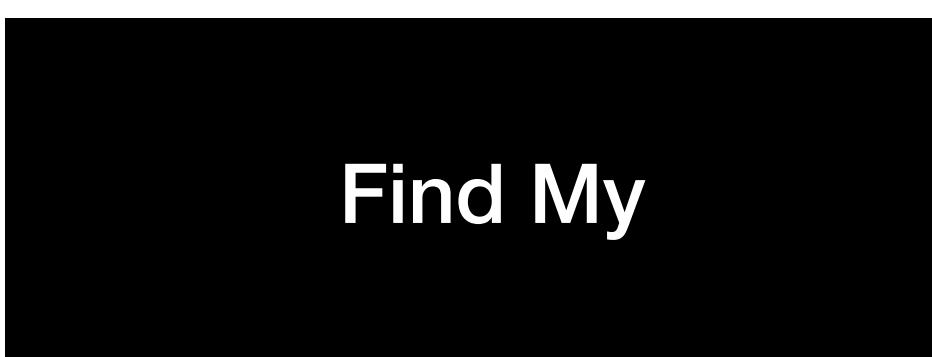
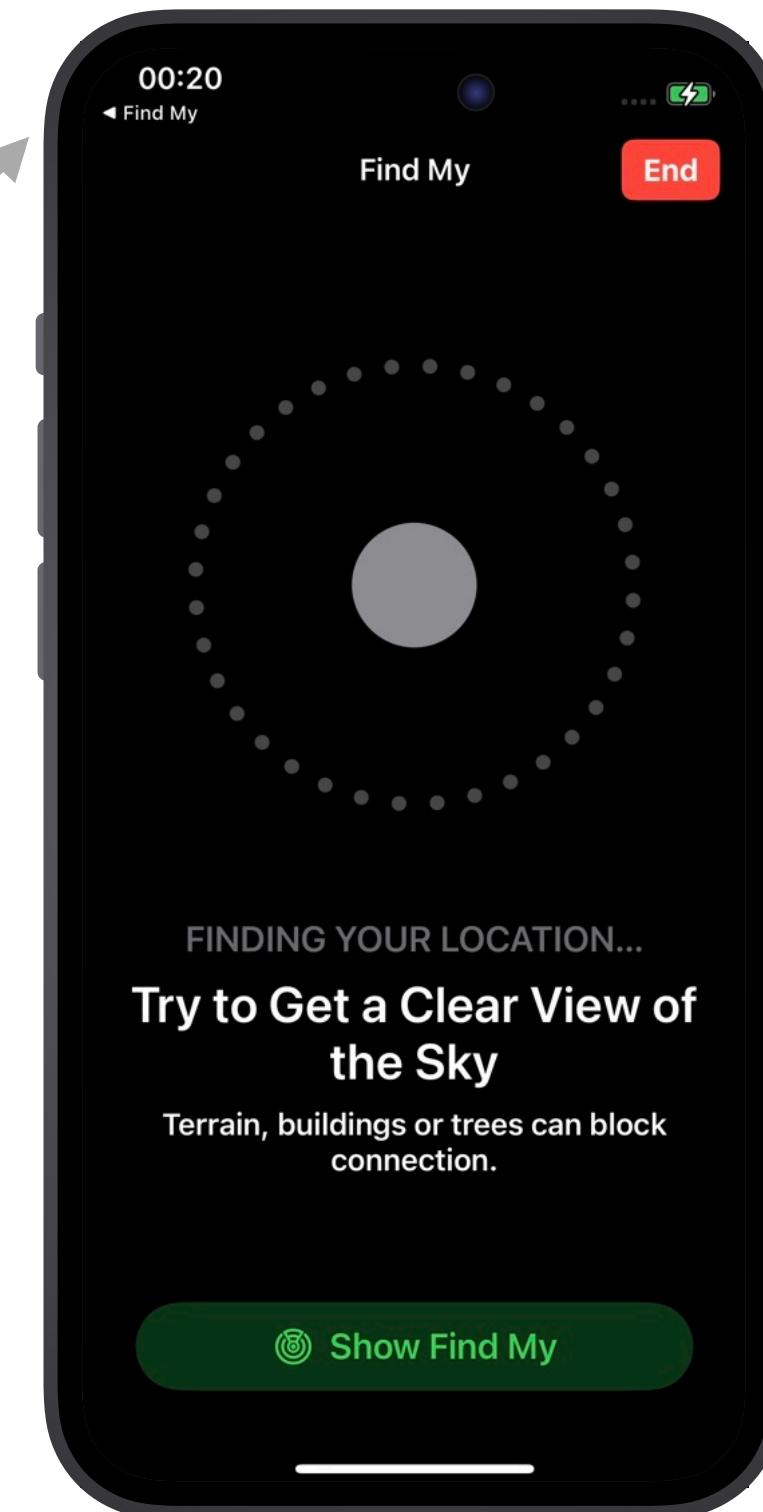




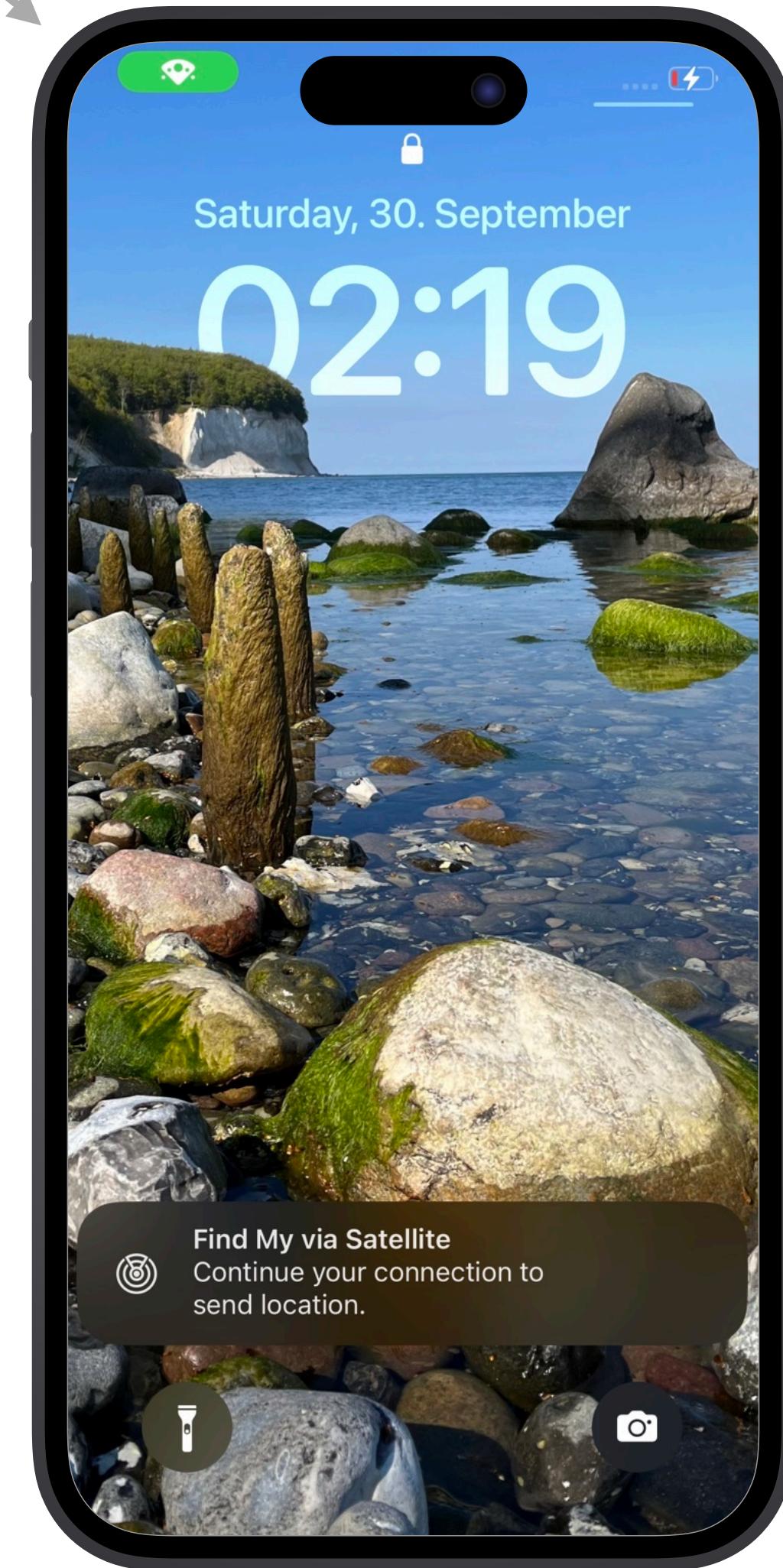
searchpartyd

XPC
com.apple.commcenter.coretelephony.xpc
requestStewieWithContext, reason=6
(FindMy)

Launch via URL
x-apple-sosbuddy://request?
reason=FindMy



Pizza icon!



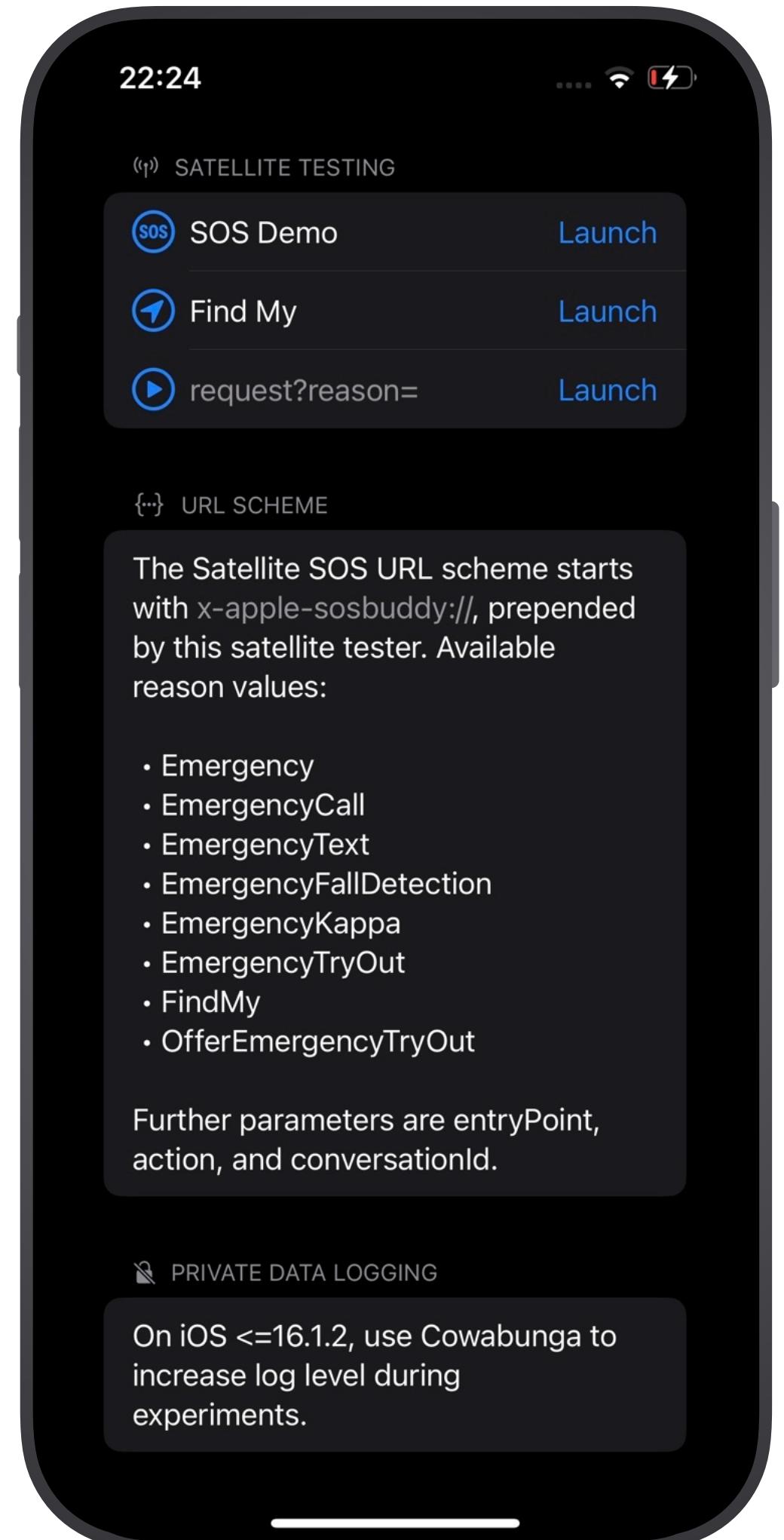
CommCenter will update involved parties upon connection updates.

Calling URLs directly?

Reverse engineer
CommCenter, build an
app for non-jailbroken
iPhone 14, ...

reason=

0. Unknown
1. EmergencyCall
2. EmergencyText
3. EmergencyFallDetection
4. EmergencyKappa
5. EmergencyTry0ut
6. OfferEmergencyTry0ut
7. FindMy
8. Test
9. Anywhere
10. AnywhereTest



Only works for
EmergencyTryOut.

Other services are not
active and are missing
state in CommCenter.

Setting custom Stewie context with reason!

XPC
com.apple.commcenter.coretelephony.xpc
requestStewieWithContext, reason=2
(EmergencyText)

Launch via URL
x-apple-sosbuddy://request?
reason=EmergencyText&conversationId=0
&action=startConversation



Frida

CommCenter

SOSBuddy

Fake it 'till you make it!



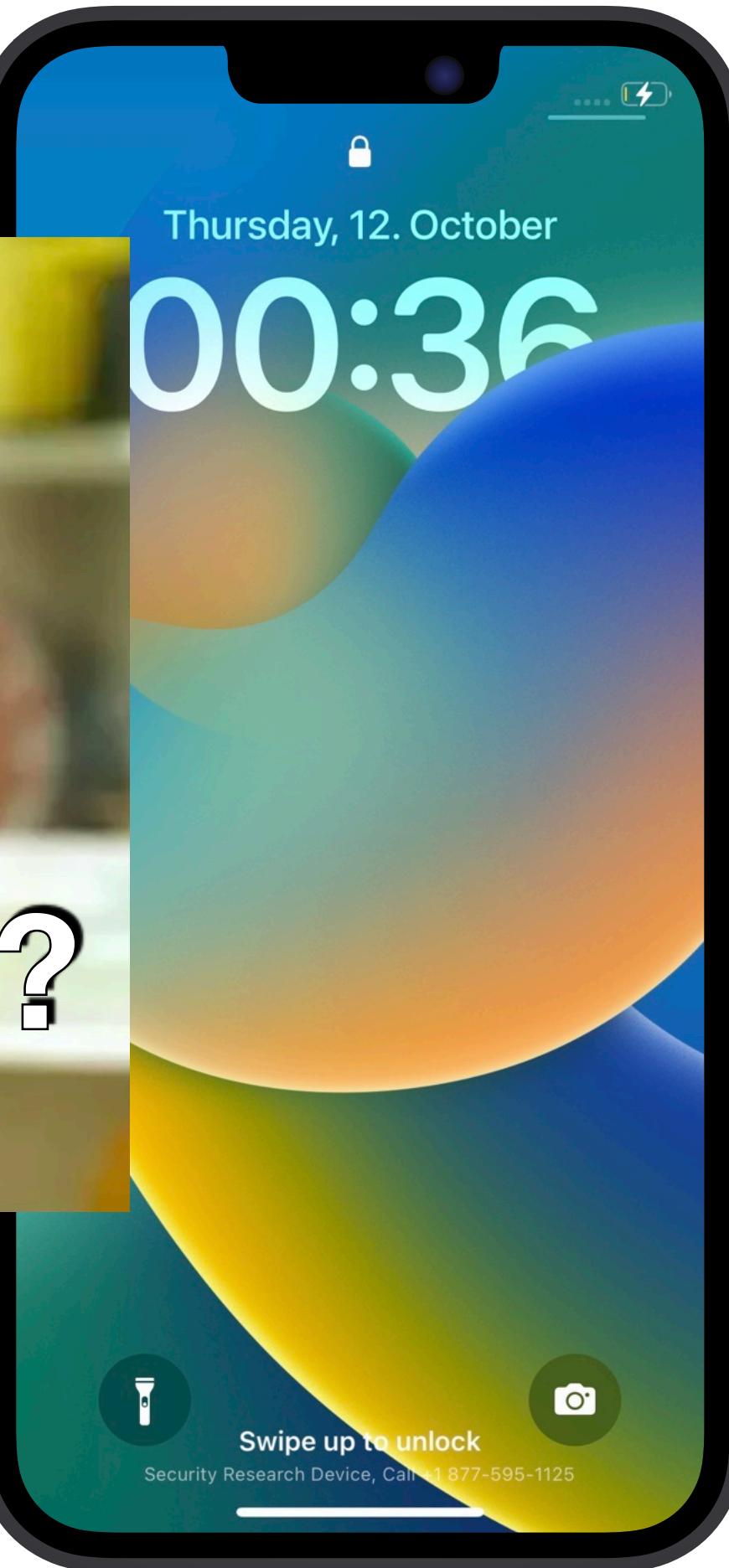


iPhone 14

No jailbreak but modem with satellite



Why not both?



iPhone 13 mini

Research device but no satellite modem

CommCenter

Initialisation
GsmRadioPersonality::create

libCommCenterBase.dylib

```
GsmRadioPersonality*
GsmRadioPersonality::GsmRadioPersonality(
    GsmRadioPersonality *this,
    shared_ptr *ptr,
    HardwareConfiguration hwconfig,
    basic_string *modelAP,
    basic_string *modelPhone)

//...

if (hwconfig >= 0x34) {
    this->bifrost_enabled_by_config =
        os_feature_enabled_impl("CoreTelephony", "Bifrost");
    this->bifrost_compatible = 1;
}

// ...
}
```

libMobileGestalt.dylib

/private/var/containers/Shared/SystemGroup/systemgroup.com.apple.mobilegestaltcache/Library/Caches/com.apple.MobileGestalt.plist

Mobile Device Properties
hwconfig=0x34
modelAP="D27AP"
modelPhone="iPhone 14, 7"

System Features
Bifrost

libsystem_featureflags.dylib

/System/Library/FeatureFlags/Domain/CoreTelephony.plist

Values as observed on
Corellium iPhone 14.

CommCenter

Parse CLI Options

```
sleep(0x10)  
sleep(0x10)
```

Attach Frida

Binary patching!

libCommCenterBase.dylib

```
const GsmRadioPersonality_create = Module.getExportByName(null,  
'_ZN19GsmRadioPersonality6createERKNSt3__110shared_ptrIK8RegistryEE21Har  
dwareConfigurationRKNS0_12basic_stringIcNS0_11char_traitsIcEENS0_9alloca  
torIcEEEESF_');  
  
Interceptor.attach(GsmRadioPersonality_create, {  
    onEnter(args) {  
        console.log(`GsmRadioPersonality::create called with hw_model=  
                  ${args[1]}, replacing with 0x34 for iPhone 14!`);  
        args[1] = new NativePointer(0x34);  
    }  
});
```

Overwriting this will screw
up CommCenter state, it
will try to load iPhone 14
baseband firmware etc.

Mobile Device Properties

hwconfig=0x34

libsystem_featureflags.dylib

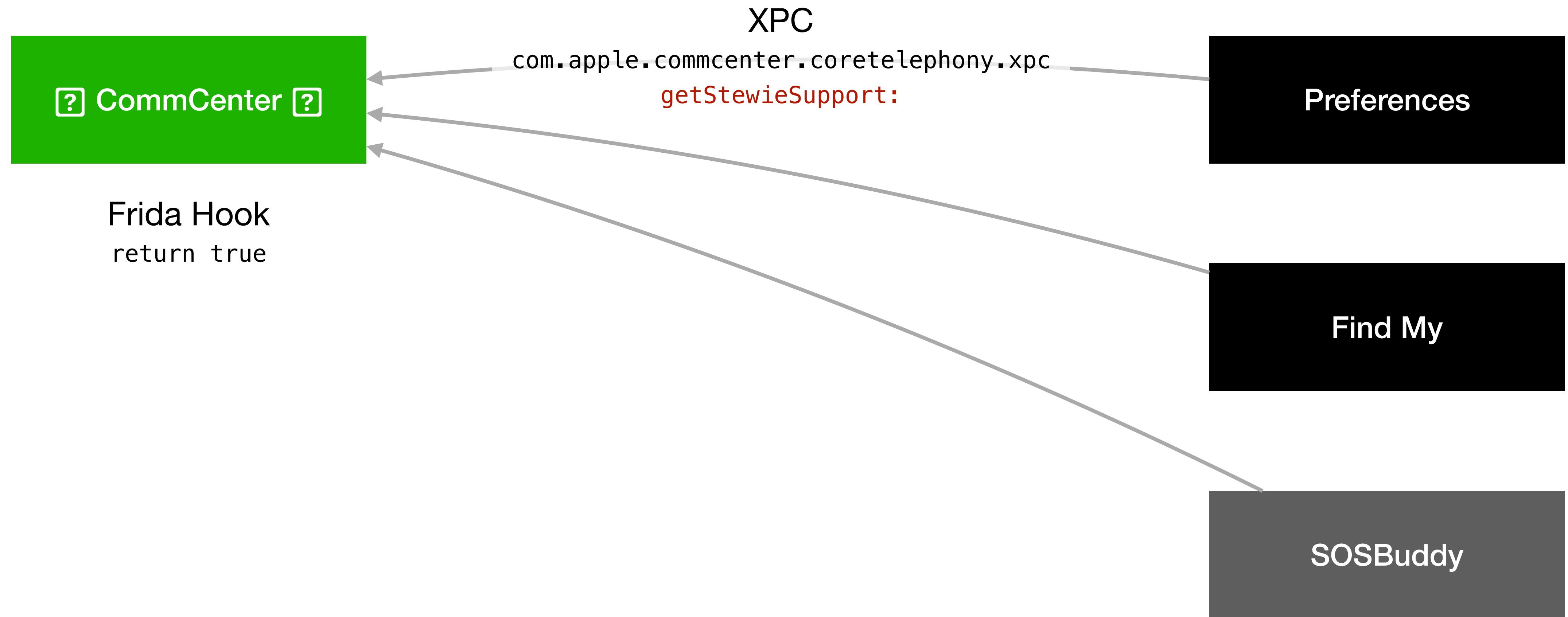
Already present on SRD.

/System/Library/FeatureFlags/Domain/CoreTelephony.plist

Applied to SRD!

/private/var/containers/Shared/SystemGroup/
systemgroup.com.apple.mobilegestaltcache/Library/Caches/
com.apple.MobileGestalt.plist

libMobileGestalt.dylib



Service Mask

CommCenter

No Cellular, no Wi-Fi?

[CTStewieState setAllowedServices:**0xc006**]

Mask Bit	Meaning
0x8000	Anywhere
0x4000	Test
0x0004	FindMy
0x0002	EmergencyTryOut
0x0001	Default

```
Interceptor.attach(requestStewieForService, {
    onEnter(args) {
        console.log(`Allowing requestStewieForService`);

        // allow all services in the 2-bytes service mask
        args[0].add(0xf2).writeShort(0xffff);

        // also allow the service right now
        args[0].add(0xf0).writeU8(0x1);
    }
});
```

...a few Frida hooks later, CommCenter will always allow all services, even outside a launch country.

Manually call SOSBuddy!

```
function openURL(url) {  
    var w = ObjC.classes.LSApplicationWorkspace.defaultWorkspace();  
    var toOpen = ObjC.classesNSURL.URLWithString_(url);  
    return w.openSensitiveURL_withOptions_(toOpen, null);  
}  
  
openURL("x-apple-sosbuddy://request?reason=OfferEmergencyTryOut")
```

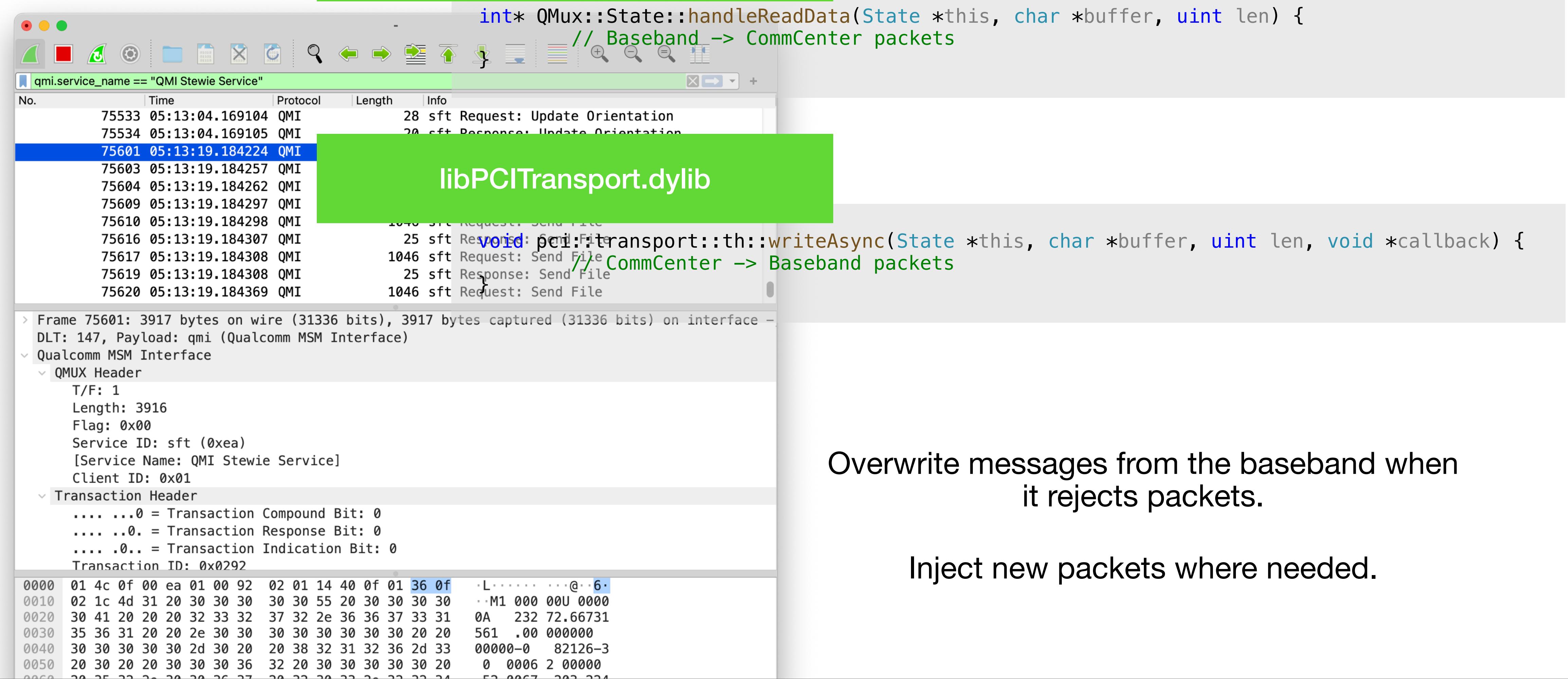
Requires iOS built with SOSBuddy.

Launch from SpringBoard with Frida.



CommCenter

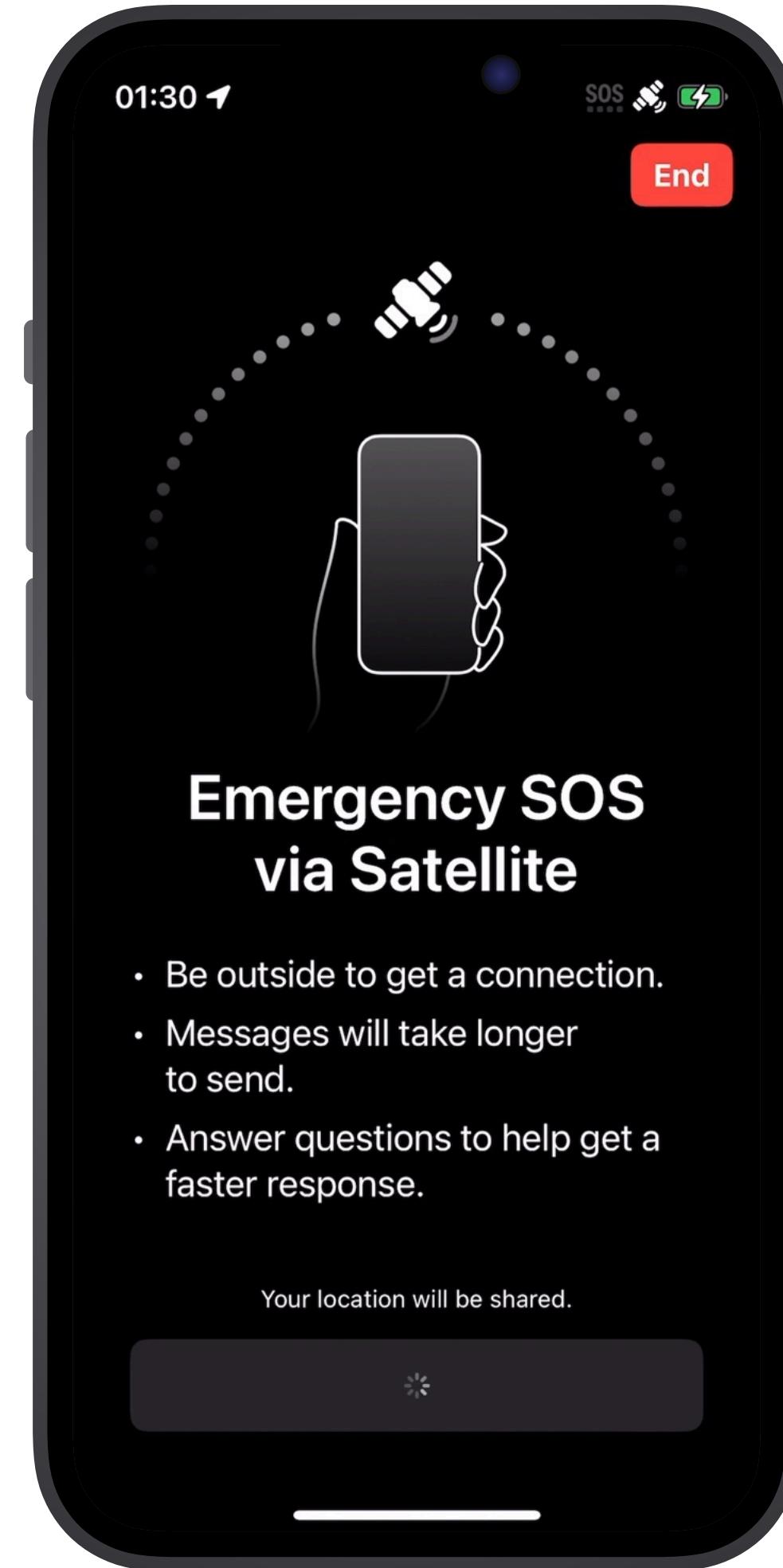
libATCommandStudioDynamic.dylib



Overwrite messages from the baseband when it rejects packets.

Inject new packets where needed.

We fake everything including satellite configs
and authentication.



Enabling Stewie on SRD allows us to analyse
the satellite ecosystem in action!

Stewie & Bifröst Configuration

What happens on-device when Stewie is available?





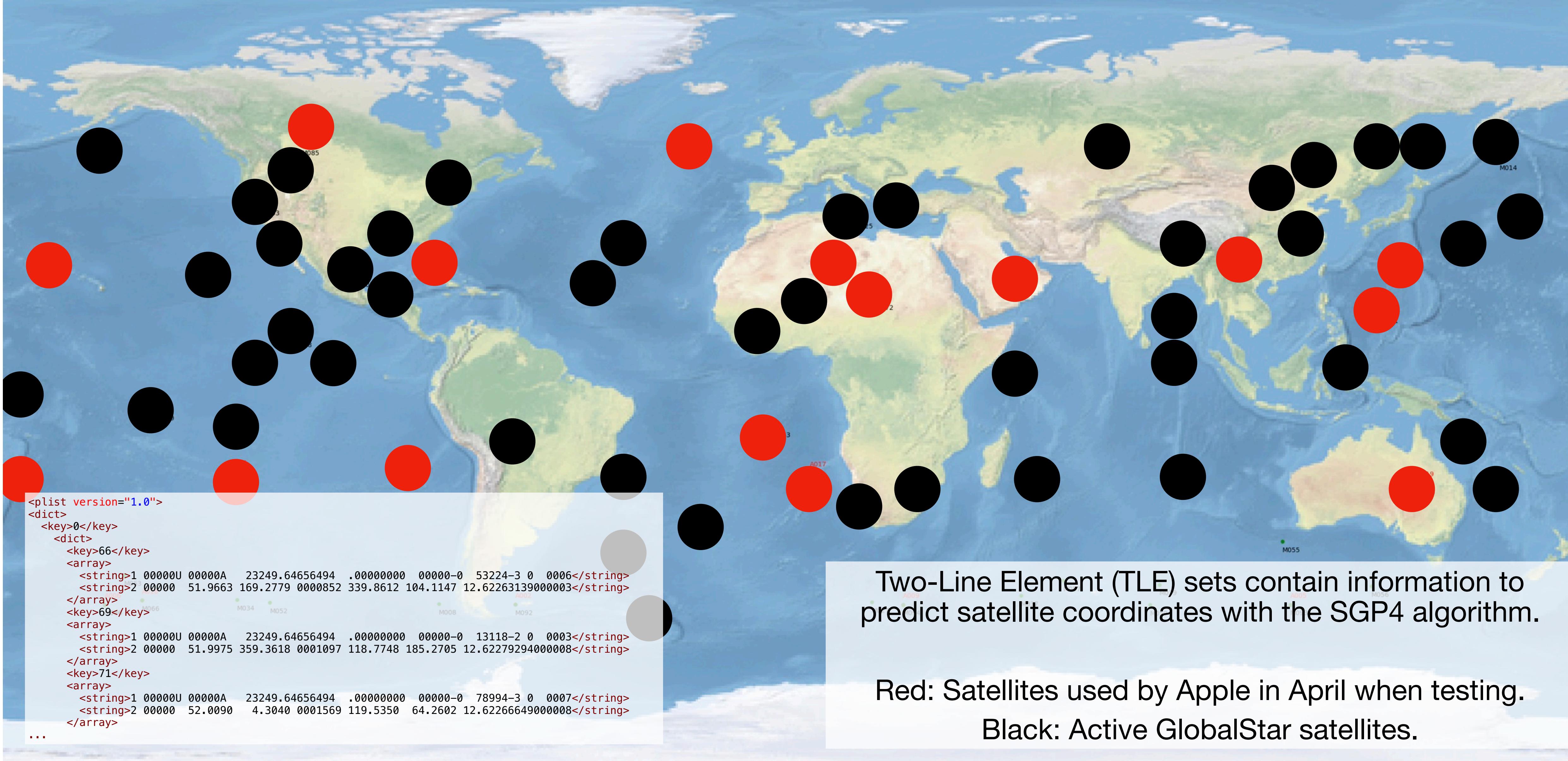
Entitlements

```
<key>com.apple.trial.client</key>
<array>
    <string>800</string>
    <string>801</string>
    <string>802</string>
    <string>803</string>
    ...
</array>
```

? /private/var/mobile/Library/Trial/Treatments/
802/factorPacks/.../assets/Targets/Targets.plist

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

CommCenter only downloads
these if Stewie is available.

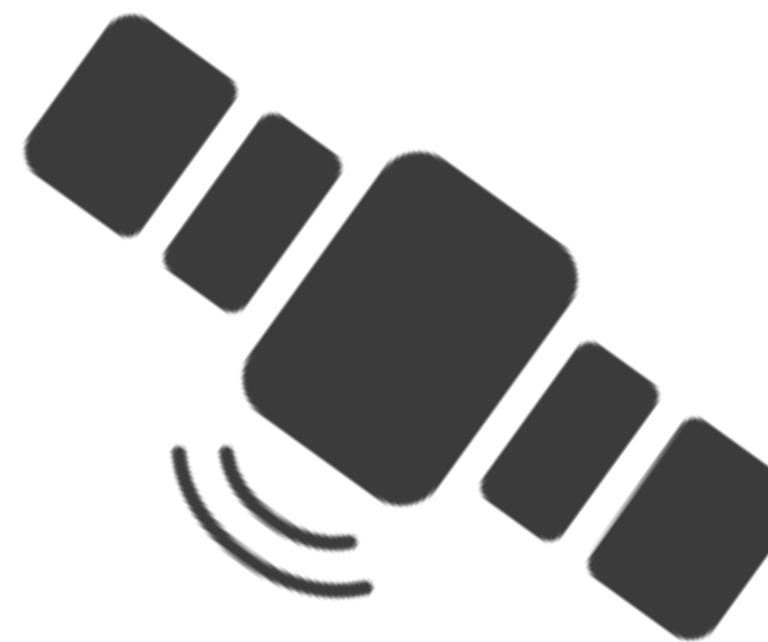


?

/private/var/mobile/Library/Trial/Treatments/
 802/factorPacks/.../assets/Targets/Targets.plist

Thanks @Fabian Portner for
 figuring this out :)

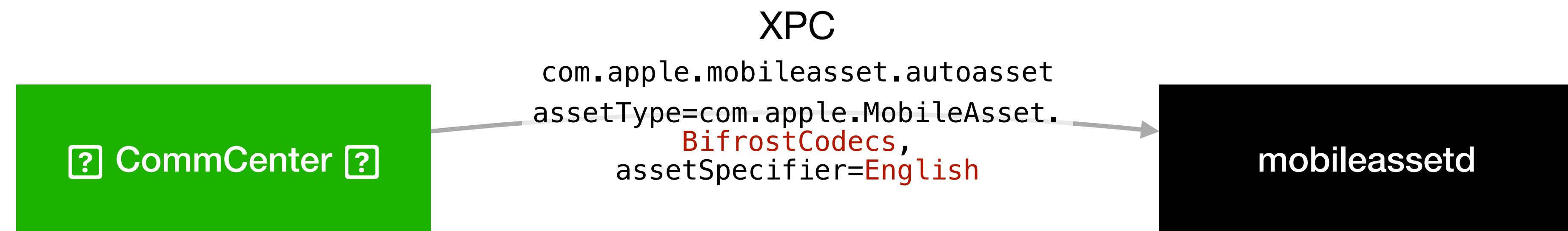
```
<plist version="1.0">
<dict>
  <key>0</key>
  <dict>
    <key>countries</key>
    <array>
      <dict>
        <key>fwd_alternate_channels</key>
        <array>
          <integer>262220</integer>
          <integer>262270</integer>
        </array>
        <key>fwd_channel</key>
        <integer>262170</integer>
        <key>iso3166_alpha_3</key>
        <string>CAN</string>
        <key>rev_channels</key>
        <dict>
          <key>nominal</key>
          <array>
            <integer>262336</integer>
            <integer>262338</integer>
            <integer>262340</integer>
            <integer>262342</integer>
            <integer>262344</integer>
            <integer>262346</integer>
            <integer>262348</integer>
```



Channel numbers, not frequencies.

?

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



Entitlements

```

<key>com.apple.private.assets.accessible-asset-types</key>
<array>
    <string>com.apple.MobileAsset.BifrostCodecs</string>
</array>
    
```

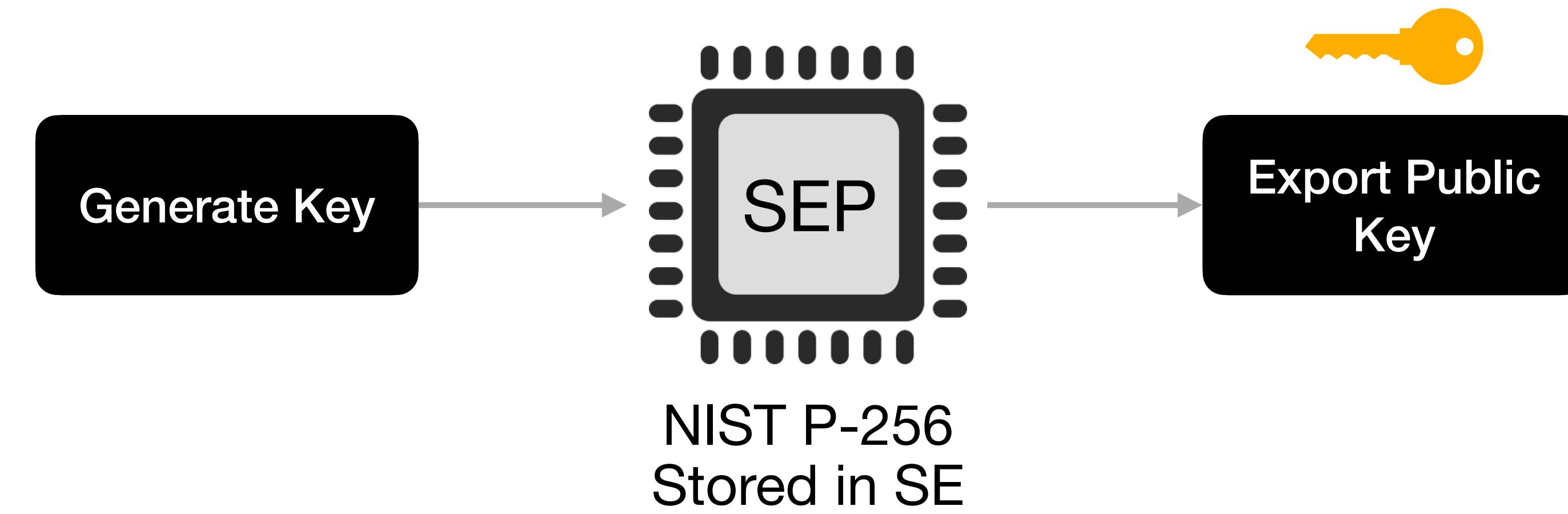
Language compression codecs used for text messaging during emergency communication.

```

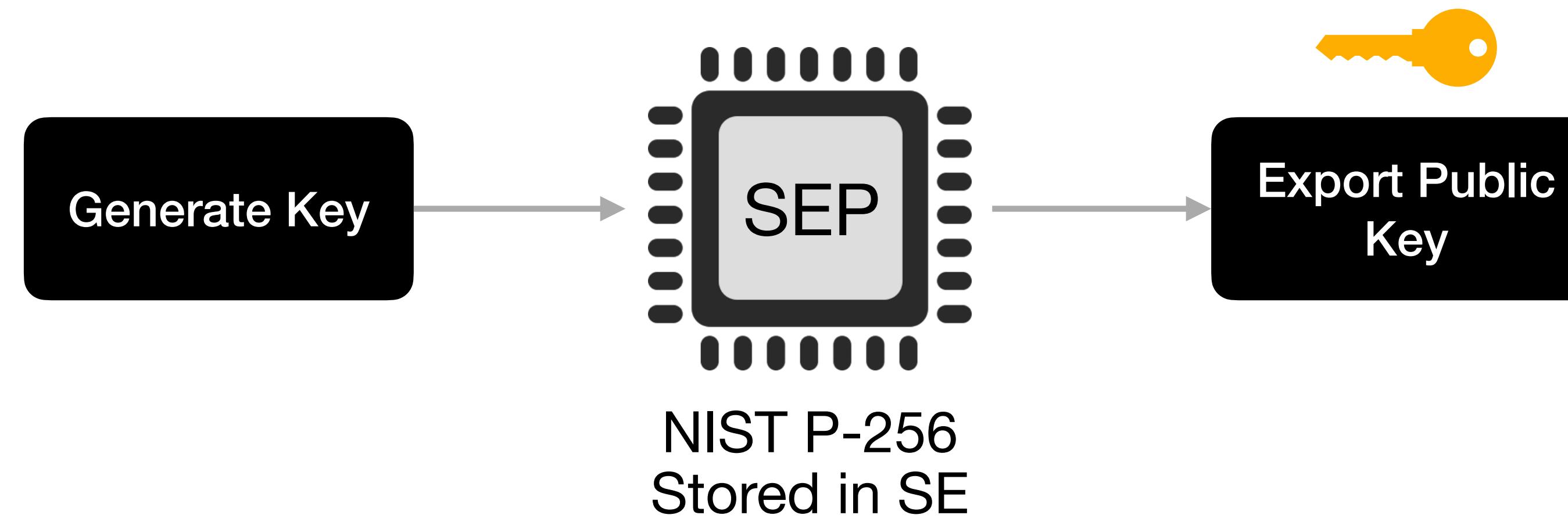
? /private/var/MobileAsset/AssetsV2/
com_apple_MobileAsset_BifrostCodecs/
purpose_auto/...asset/AssetData/codec
    
```

00000000	01 00 00 00 01 00 05 00	80 00 f0 f0 f0 80 b5 c0	•000•0•0 •0xxxxxx
00000010	00 70 60 70 80 80 10 00	f0 80 60 70 a0 60 70 40	0p`p×x•0 •xx`p×`p@
00000020	80 80 45 80 00 30 d0 80	80 00 80 80 20 70 60 50	xxEx00xx •x0xx p`P
00000030	70 60 90 00 70 80 90 00	b5 80 80 80 4b bb 80	p`x0p×x0 •xxxxxKxx
00000040	00 f0 10 00 00 f0 80 4b	80 80 00 80 80 80 80 80	0x•00xxK •xx0xxxxx
00000050	30 90 60 80 80 70 a0 90	70 70 10 90 b0 80 00 d0	0x`x×pxx pp•xxx0x
00000060	70 80 40 70 a0 60 00 a0	80 bb 41 b1 80 36 b1 b7	p×@p×`0x •xxA×x6xx
00000070	80 80 80 80 41 80 80 80	f0 00 80 f0 00 e0 00 26	xxxxAxxxx •0xx0x0&
00000080	fd 7d 60 f0 ed 49 55 d5	80 b9 fd 80 d0 b3 80 69	x}~xxIAUx •xxxxxxxi
00000090	55 80 80 80 80 41 5d 4b	10 70 00 70 10 10 90 30	UxxxxxAJK •p0p••0
000000a0	f0 60 70 70 70 20 f0 f0	f0 70 50 90 90 60 80 90	x~ppp xx •xpBxx`xx
000000b0	10 b0 40 f0 f0 20 50 70	f0 70 60 70 80 80 80 90	•x@xx Pp •p`pxxxx
000000c0	10 a0 30 e0 f0 00 00 00	80 50 8e 5e c7 e5 be 80	•x0xx000 xPx^xxxx
000000d0	30 37 80 a5 be 60 14 80	80 80 37 ed 89 35 87 67	07xxx~•x •x7xx5xg
000000e0	4e 80 17 80 80 80 80 c7	80 00 40 80 a0 80 80 20	Nx•xxxxx •x0xxxxx
000000f0	10 80 27 e0 60 bd 15 ce	40 00 e0 80 e0 d0 0b f0	•x' x~x•x •@0xxxxx•x
00000100	40 00 80 80 f0 f0 30 c7	eb 30 80 70 c6 80 47 80	@0xxxxx0x •x0xp×xGx
00000110	37 80 80 c0 1b 80 90 60	80 64 b6 30 80 80 80 80	7xxx•xx •xd0xxxx
00000120	80 40 48 c8 60 a0 8e c0	80 80 80 1b a0 80 e0 20	x@Hx` xxxx •xx•xxx
00000130	80 42 62 80 80 e5 80 80	ad 4d 80 42 80 80 80 80	xBbxxxxx •MxBxxxx
00000140	80 80 80 80 80 42 b3	00 80 30 f0 80 b0 30 d0	xxxxxxBx •0x0xx0x
00000150	39 c9 80 80 c9 80 80 80	67 eb 70 8c b2 20 74 80	9xxxxxx gpxx tx
00000160	f4 80 80 80 2c 54 80 80	80 80 80 80 80 04 9c	xxxxx,Txx •xxxxxx•x
00000170	48 b8 14 80 48 80 46 80	30 48 80 80 39 80 48 4d	Hx•xHxFx •OHx9HM
00000180	04 e5 80 ce 80 4c cc 97	b2 42 80 b2 80 80 80 80	•xxxxxLxx •xBxxxxxx
00000190	70 42 80 80 c0 80 80 00	48 80 80 80 b2 80 80 c0	pBxxxxx0 Hxxxxxx
000001a0	80 1e 1e 80 64 80 40 80	80 1e 07 f7 80 80 f7 80	•x•x•d@x •x•xxxxxx
000001b0	80 00 f0 d0 77 f0 eb b0	80 40 10 00 80 20 80 e7	x0xxwxxx •x@0xx x
000001c0	37 b8 40 80 4e ee 00 80	80 80 80 80 3f 3f 80 cf	7x@Nxx0x •xxxxx?xx
000001d0	80 80 80 80 20 80 e7 37	80 80 80 b8 f0 3f 80 80	xxxxx xx7 •xxxxx?xx
000001e0	80 42 b2 80 80 80 4b 4b	4e bb 80 8f 5f 30 4b 9f	xBxxxxKK Nxxxxx_OKx
000001f0	80 80 80 80 30 2f 80 4b	40 02 82 80 eb e2 80 80	xxxxx0/K •@•xxxxxx
00000200	df 1b 80 5b e7 c7 80 bb	80 f0 1b 80 80 4b 56 f6	•x•x[xxx] •xx•xxKVx
00000210	ec 80 e6 3f 48 80 80 2f	56 80 80 80 1b 80 80 80	xxxx?Hxx/ Vxxxxx•xx
00000220	3e 3e 80 8e c6 71 89 79	3e e9 c9 80 80 4b 49 11	>>xxxqxy >xxxKI•
00000230	a9 3e 80 3e 80 42 aa 5a	3e 76 ea 80 56 80 80 42	x>x>xBxZ >vxxVxxB
00000240	5a 80 ce 3e df 80 80 80	35 99 b2 80 9a 80 80 80	zxx>xxxx 5xxxxxx

LLC Keys



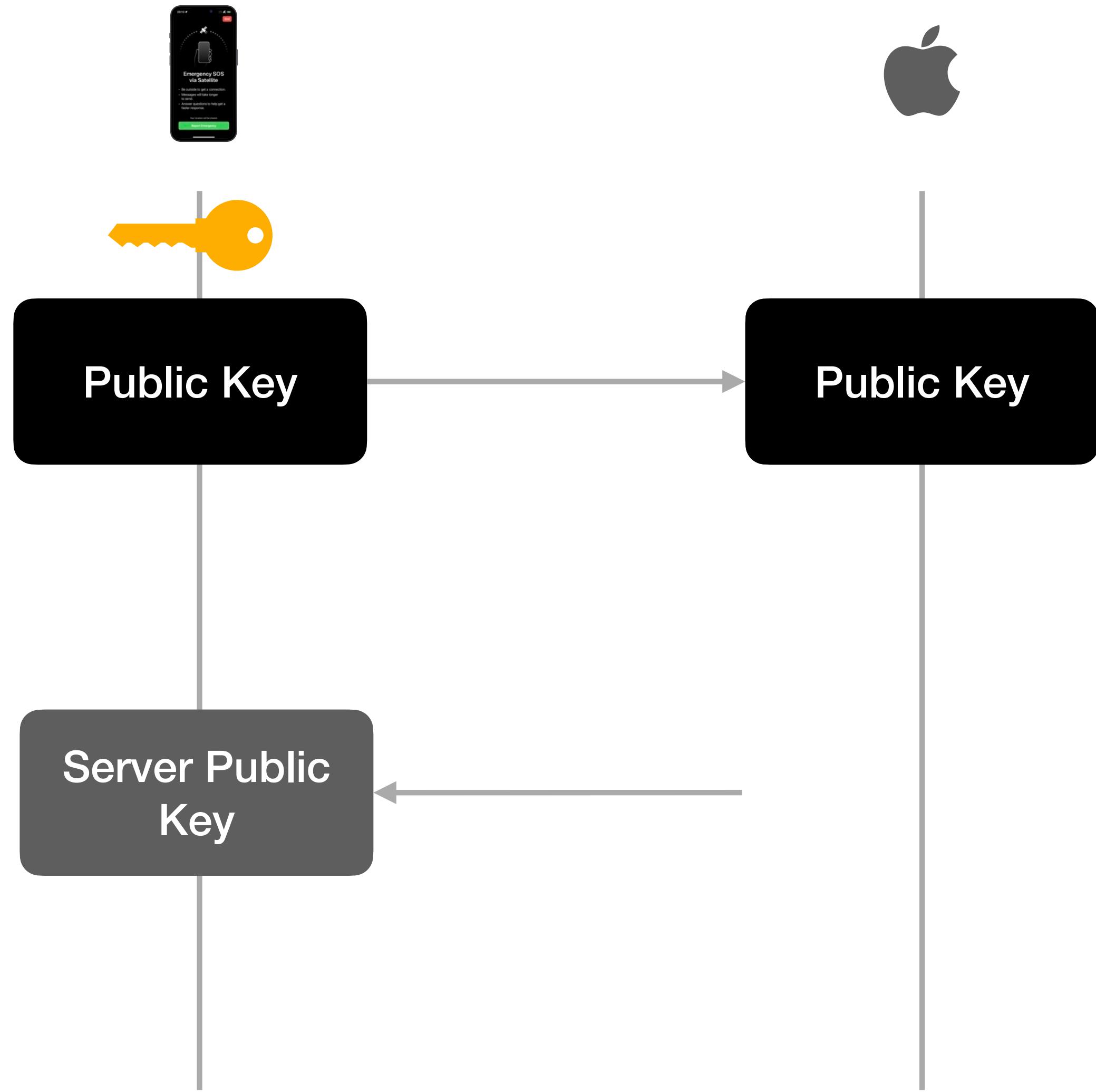
LLC Keys



```
var keyAttributes = NSMutableDictionary()
keyAttributes[kSecAttrLabel] = "com.apple.commcenter.llc"
keyAttributes[kSecAttrTokenID] = kSecAttrTokenIDSecureEnclave
keyAttributes[kSecClass] = kSecClassKey
keyAttributes[kSecAttrAccess] = kSecAttrAccessibleAlwaysThisDeviceOnly
keyAttributes[kSecAttrIsPermanent] = true
keyAttributes[kSecAttrKeySizeInBits] = 256
keyAttributes[kSecPrivateKeyAttrs] = kSecAttrKeyTypeECSECPrimeRandom

var error: NSError?
let success = SecKeyCreateRandomKey(keyAttributes, &error)
```

Key Synchronisation

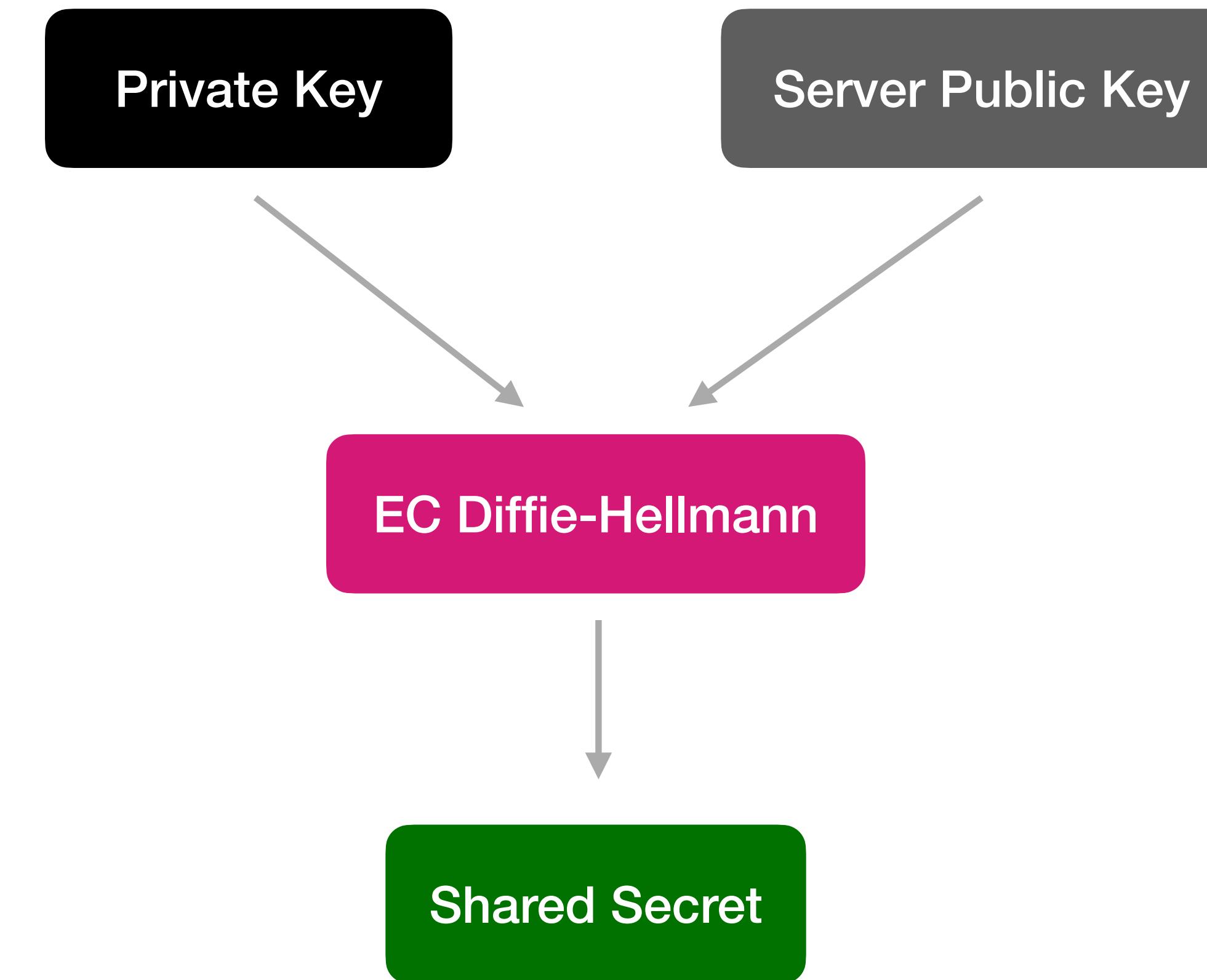


iOS Keychain

```
{  
    agrp = apple;  
    bsiz = 256;  
    decr = 0;  
    drve = 1;  
    encr = 0;  
    esiz = 0;  
    extr = 0;  
    kcls = 1;  
    klbl =  
        0xedede4c2fa65c88fe965720d719ea80c5e8  
        39195d8  
    labl = "com.apple.commcenter.llc";  
    perm = 1;  
    priv = 1;  
    sign = 1;  
    sync = 0;  
    sysb = 1;  
    tkid = "com.apple.setoken";  
}
```

```
{  
    acct =  
        "com.apple.commcenter.Stewie.STKData.  
        ede4c2fa65c88fe965720d719ea80c5e839  
        195d8";  
    agrp = apple;  
    labl = "com.apple.commcenter.llc.stk";  
    svce = CommCenter;  
    sync = 0;  
    "v_Data" = {length = 109, bytes =  
        0x62706c69 73743030 4f104104 4914d1f9  
        ... 00000000 0000004c };  
}
```

Session Key



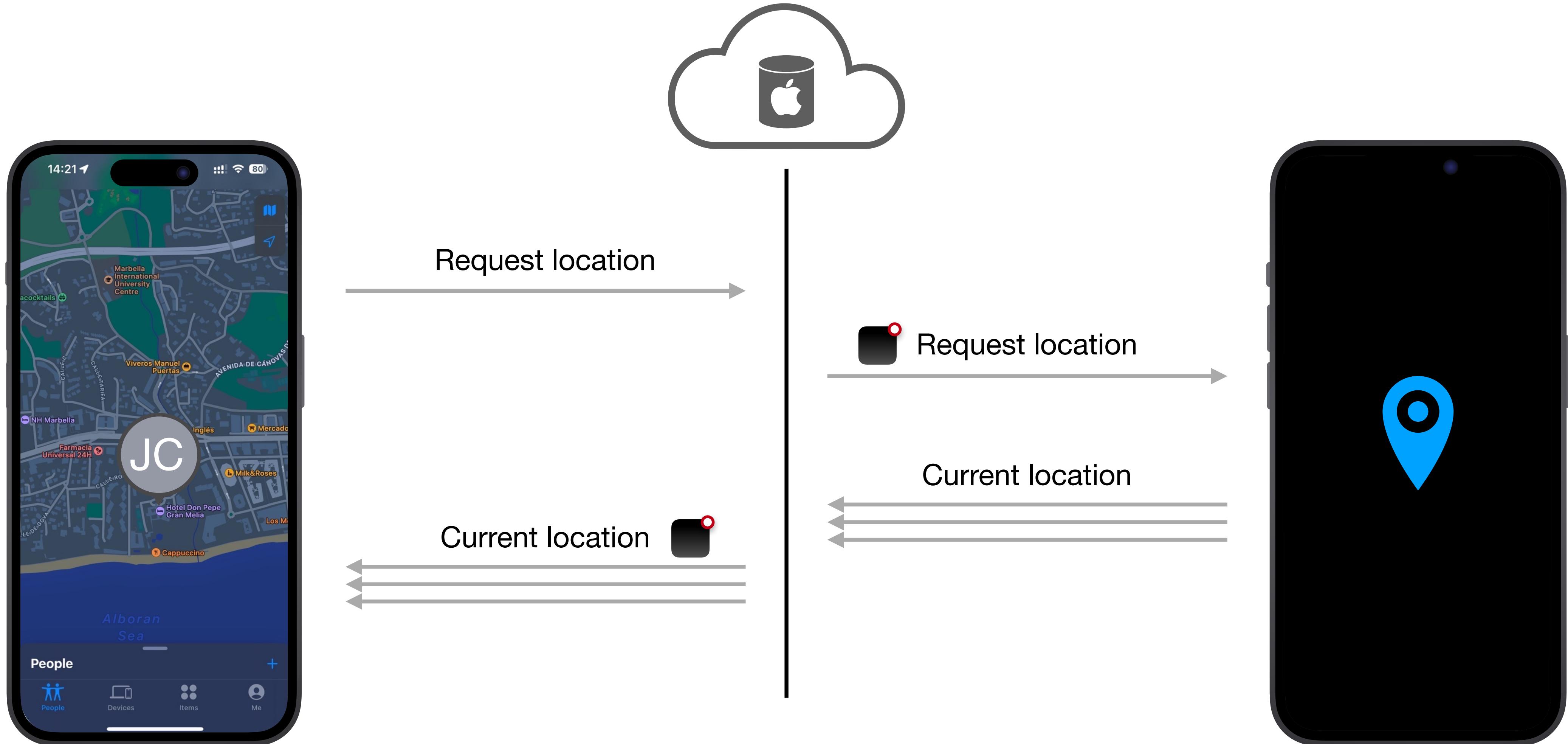
EPKI:%s, SECRET:%@

unable to generate shared secret for EPKI:%s
and LBL [%@], error

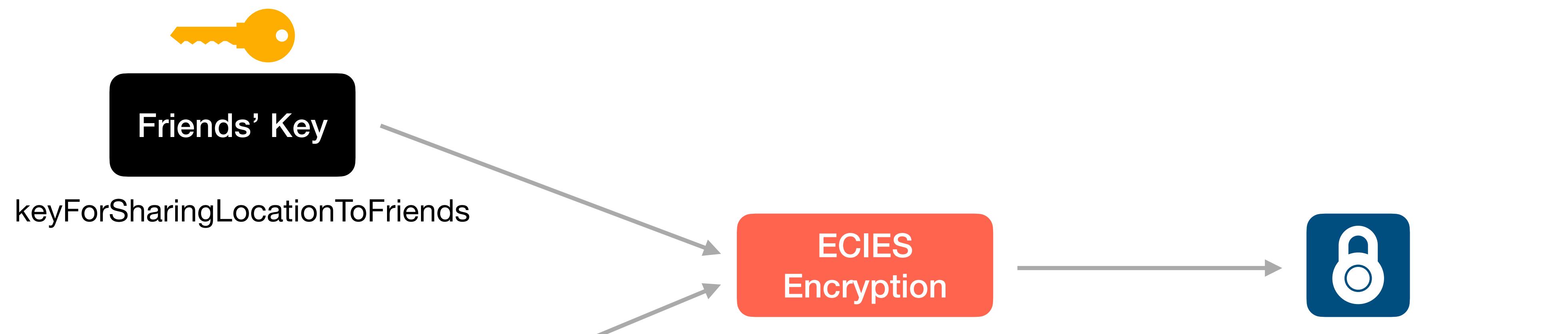
A photograph of a woman with blonde hair, wearing a tan trench coat and a grey scarf, walking down a city street at night. She is looking down at her smartphone. The background is blurred, showing other people walking, city lights, and a traffic light. The overall atmosphere is urban and focused on technology.

Find My Location Sharing

Normal location sharing



End-to-End Encryption



eciesEncryptionStandardVariableIVX963SHA256AESGCM

Server Communication

Request

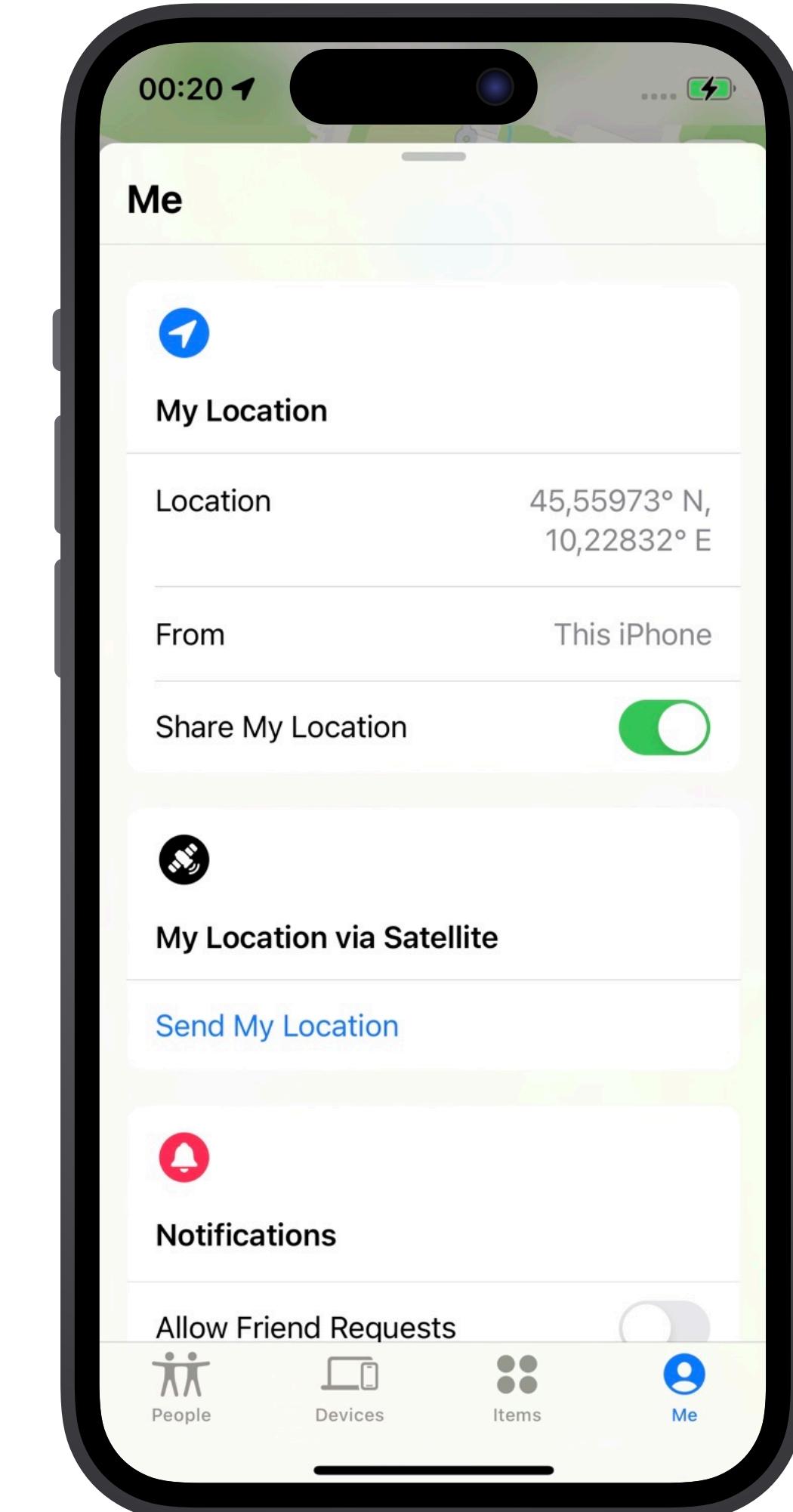
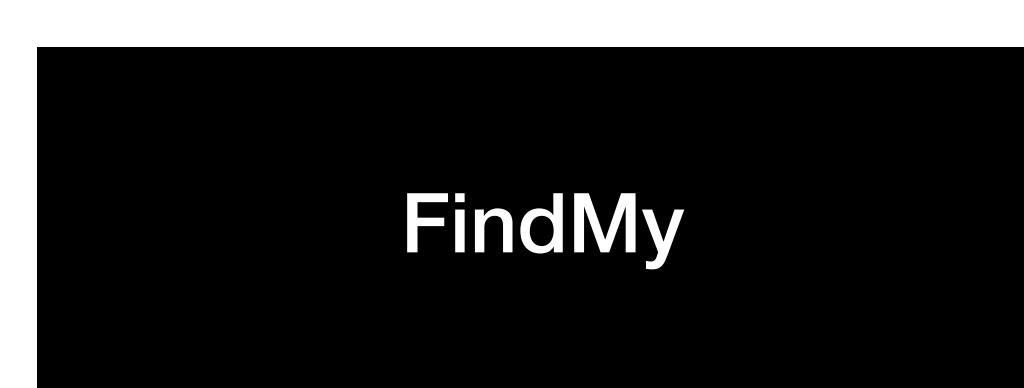
```
{  
  "fetch": {  
    "intent": "startLocationUpdates",  
    "fmId": "NDMxNjY2NDIx",  
    "mode": "live",  
    "ids": [  
      "5832C58C5C48CEF1C27D3DF1552707FE42745B966AD75BA51D04B  
      7B34A698CD2"  
    ]  
  },  
  "clientContext": {  
    "apsToken":  
      "5832C58C5C48CEF1C27D3DF1552707FE42745B966AD75BA51D04B  
      7B34A698CD2",  
    "contextApp": "com.apple.findmy.fmfc",  
    "clientId": "00008110-000260C02640011E",  
    "shallowStats": {}  
  }  
}
```

Response

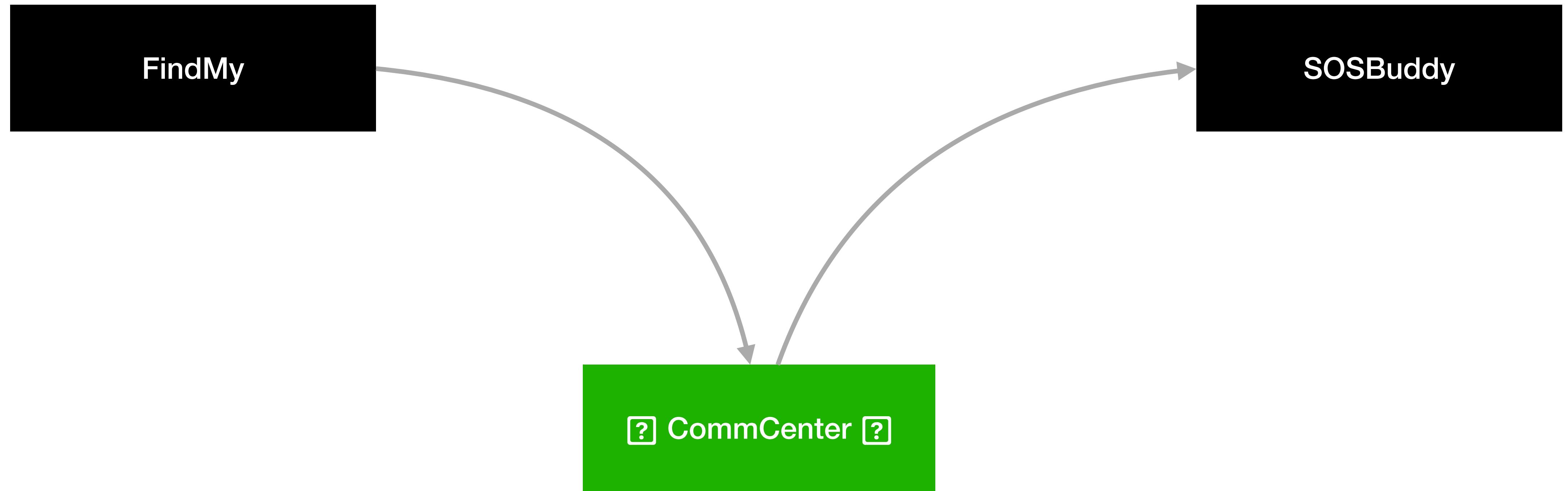
```
{  
  "locationPayload": [  
    {  
      "locationInfo": [  
        {  
          "locationTs": 1694186159999,  
          "location":  
            "BFoX1TnSgzckVvD8mRxBGWLQFFJAKkTnzd0HAZZLCdvyan8M+E6GpiHSN6gQnmRV  
            n7IBY7DQslaBGRNUJPdU+4Reyk0KDqYg807DrIVgb+0WLwgH1IYBtGIUv8Cd1GHn3  
            FxePeP1LJYn4vEDQoA2zUervtNEfsM6zU4McUipF1aHg4x//  
            sKU6mxekrQ+r+0MiBkfA0yAyGKbjfaLv+fy9ZNLnuFKVAtjqywLDgedZK4q43RbYD  
            ksdaZ0Bvlp6jql7qoaoUZfH1owVWccm9aRcrZtARa/j/UIRR3ClhQSYCRutq/  
            gubxqo27gy+5wluhM7GLB5dwn0KPJkP+kVWN0j5EvXAPxQaSnoYicI0wLhgDhwj/  
            wrZaqYnsr9Listjh/  
            5j+DAvtKVZARD4x+RDvdhabiF1Y9vrX2SG9+3KX+QXrjQ+6k+vtm6mAp+ihEj/  
            lABAHknYkwZKT88m4CGK48pDLkCCh/  
            1A3EARimdVAcUN0Yj7AbzPEb9PiTA2+v8eEtWPrKtY606w48P4Ul",  
            "fmt": 0  
        }  
      ],  
      "id": "9Cx1EA8ublnacqnTQAsdsAp4g0cmp13nipiEAVniu0o="  
    }  
  ],  
  "configVersion": 21,  
  "statusCode": "200"  
}
```

Satellite Location Sharing

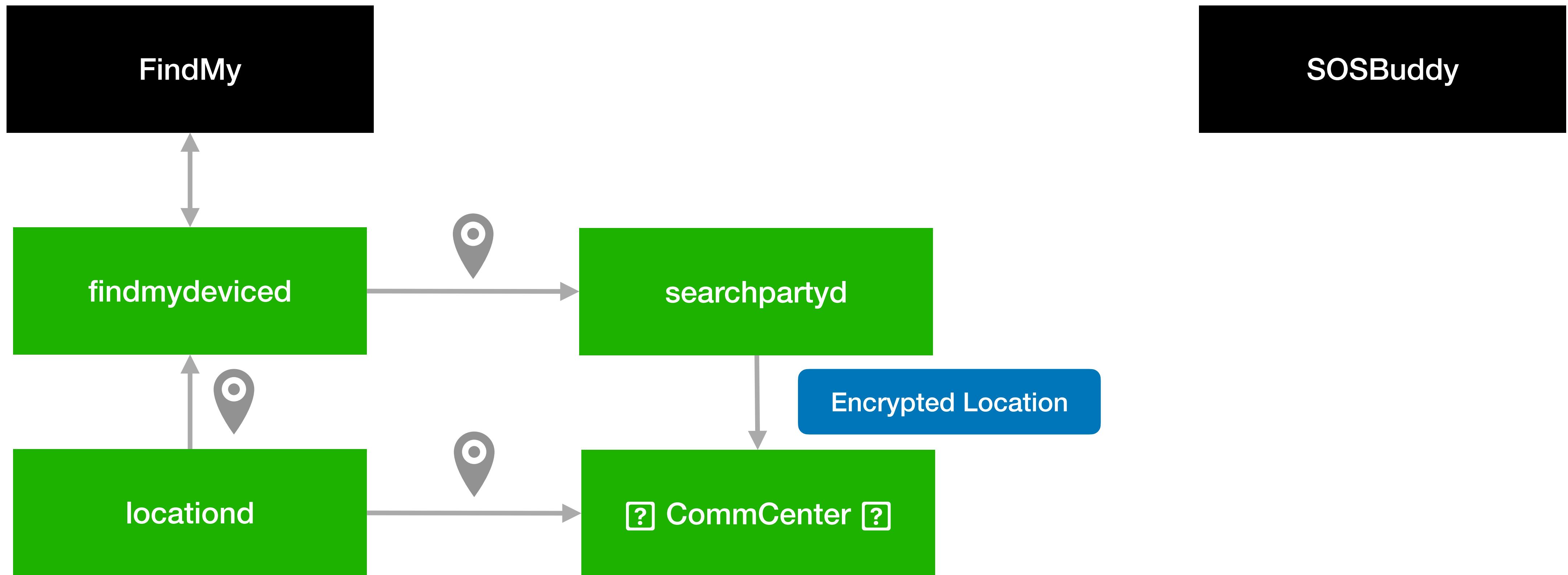
Involved Processes



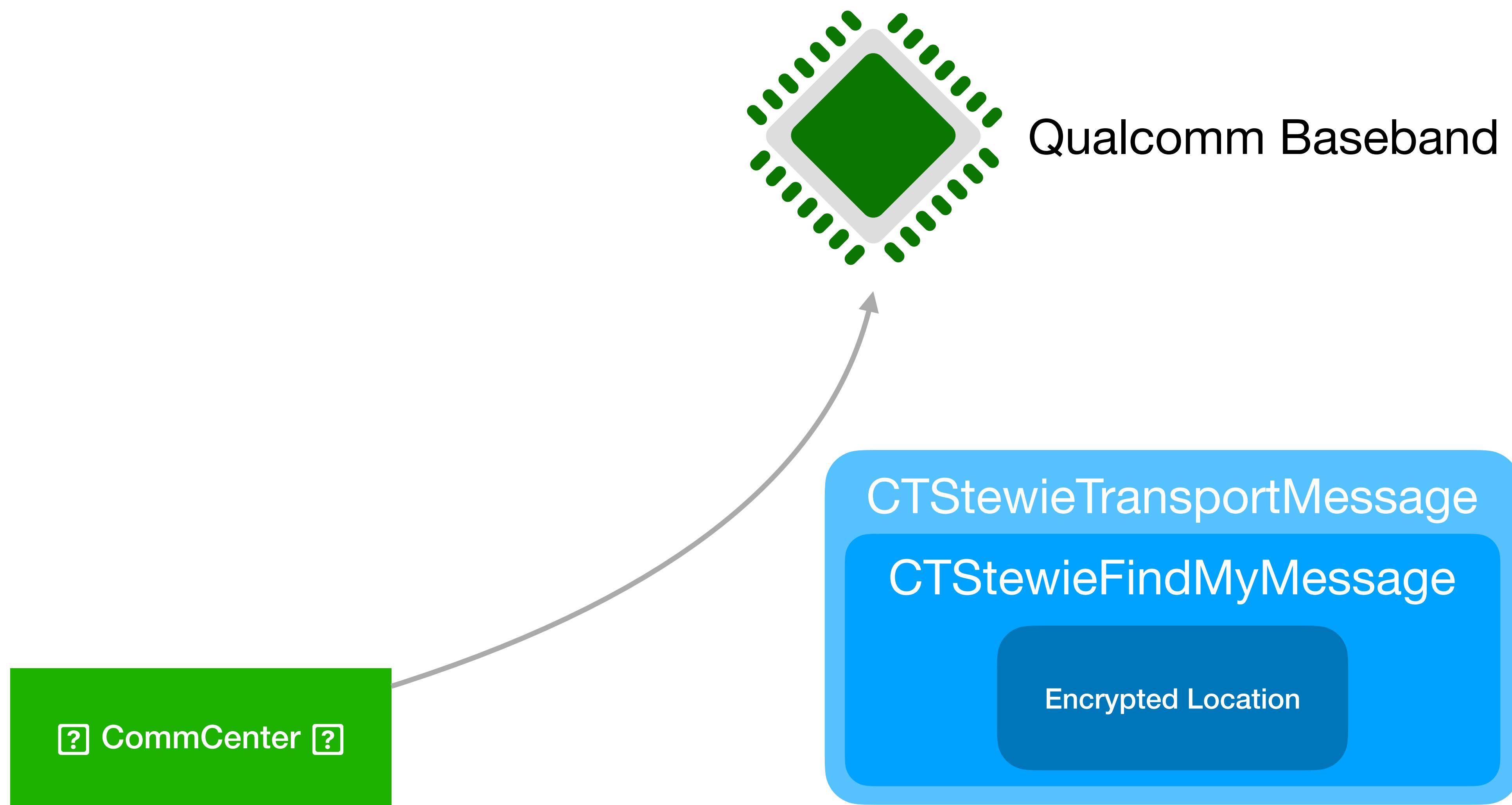
Involved Processes



Involved Processes



Involved Processes



Satellite Transmission

Reducing Data Size

Lite
Location

Satellite Transmission

`Int32(latitude * 10,000,000)`

`+`

`Int32(longitude * 10,000,000)`

`+`

`UInt8(horizontalAccurazy)`

`=`

Lite
Location

9 bytes

Satellite Transmission

```
Int32(latitude * 10,000,000)  
+  
Int32(longitude * 10,000,000)  
+  
UInt8(horizontalAccuracy)  
=
```

Lite Location 9 bytes

48.431139

4843113900

08.656773

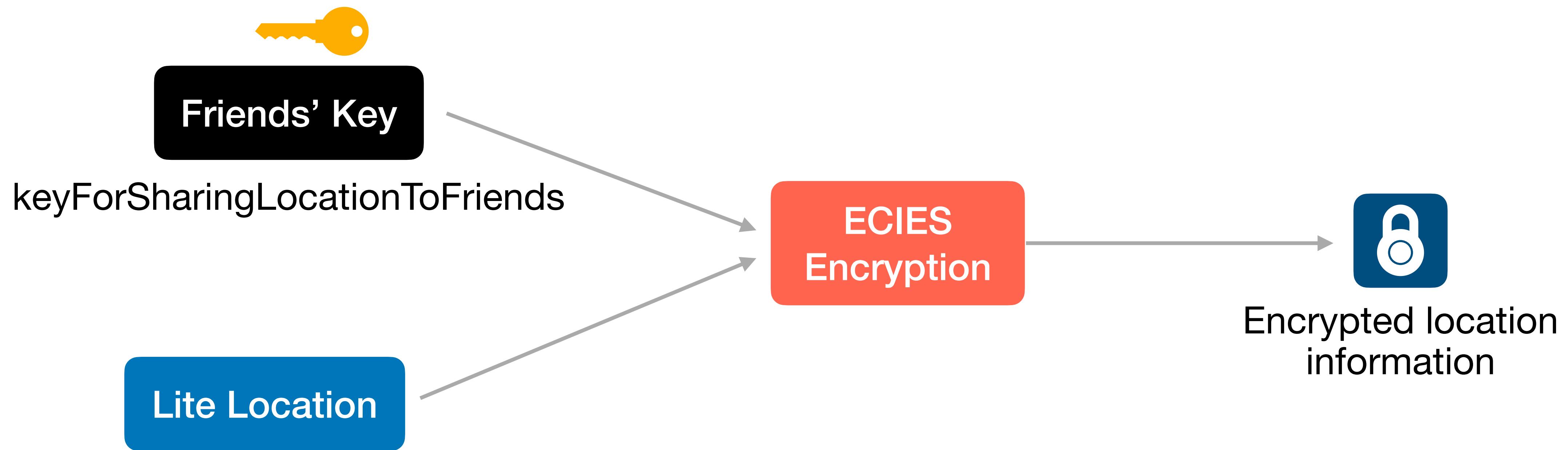
865677300





AirTag

Satellite Transmission



Satellite Transmission



Misuse



Misuse of Satellite Communication

Sending Messages for Free

- Satellite messages are expensive
- Location sharing can only be used every 15 minutes
- Bandwidth is limited
- Millions of users

Manipulating the Location

...to send messages

Latitude : -90.0 - 90.0

Longitude: 0.0 - 180.0



Manipulating the Location

...to send messages

Latitude : -90.0 - 90.0

Longitude: 0.0 - 180.0



8 bytes of data

Mapping the Alphabet

...on GPS Coordinates

A-Z a-z 0-9

62 chars

10,000,000,000

10 digits space

2 digits = 1 char

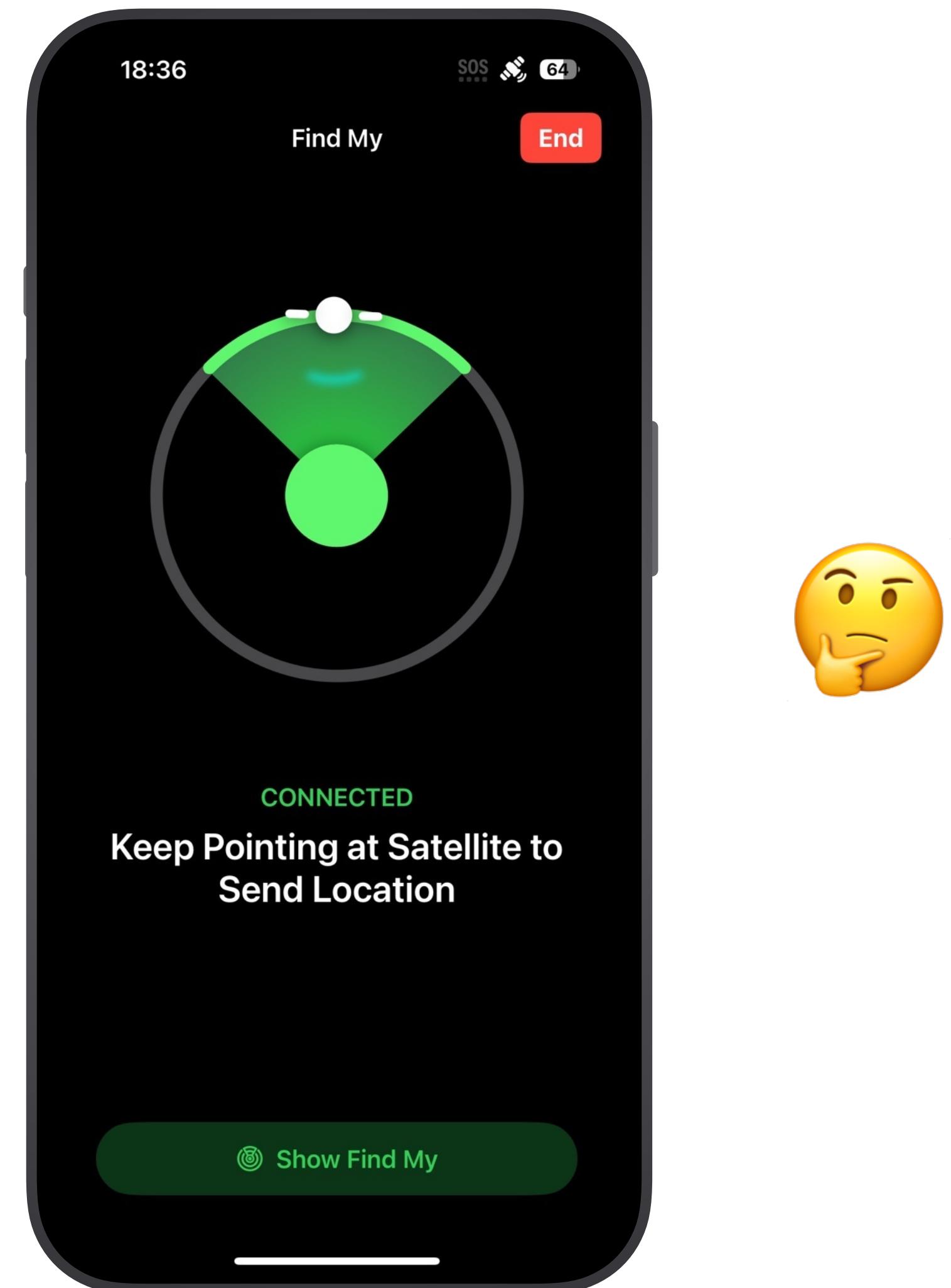
5 chars per coordinate

HelloWorld

10 characters per message

Apple was smarter!

CommCenter has checks if
location source was simulated



ios 16 jelbrek for iphone 14, wen eta?



Jiska Classen

Group Leader

Hasso Plattner Institute

jiska.classen@hpi.de



Alexander Heinrich

Security Researcher & PhD Candidate

Technical University of Darmstadt

aheinrich@seemoo.de

Image Sources

- Slide 2,4,8,12,14,42,52: Generated by Midjourney
- Slide 9: Pixabay
- 11: findmespot.com (official product image)
- Satellites, iPhone frames, processor chips are self drawn