



Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

Hacking DOCSIS

Joel Stein

Hacking DOCSIS

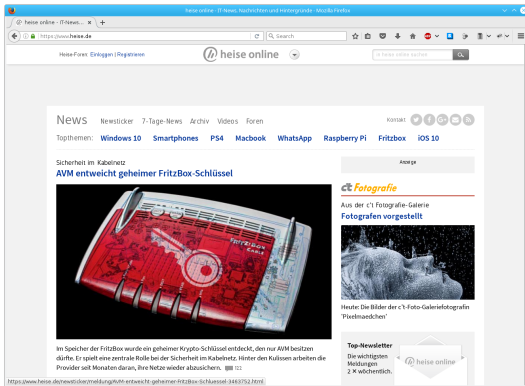
Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"




The screenshot shows a web browser window displaying a news article on the Heise online website. The article is titled "AVM entweicht geheimer FritzBox-Schlüssel" (AVM leaks secret FritzBox key) and is categorized under "Sicherheit im Kabelnetz" (Security in cable network). The article features a photograph of a red Fritz!Box router with a red key symbol overlaid on it. The text of the article discusses the discovery of a secret cryptographic key stored in the router's memory, which is used for security in the cable network. The article is dated 11.11.2016. The browser's address bar shows the URL "https://www.heise.de".

News Neusticker 7-Tage-News Archiv Videos Foren Kostenlos 🔍 🔒 📄 📧

Topthemen: [Windows 10](#) [Smartphones](#) [PS4](#) [Macbook](#) [WhatsApp](#) [Raspberry Pi](#) [Fritzbox](#) [iOS 10](#)


Sicherheit im Kabelnetz
AVM entweicht geheimer FritzBox-Schlüssel



Im Speicher der FritzBox wurde ein geheimer Krypto-Schlüssel entdeckt, den nur AVM besitzen dürfte. Er spielt eine zentrale Rolle bei der Sicherheit im Kabelnetz. Hinter den Kulissen arbeiten die Provider seit Monaten daran, ihre Netze wieder abzusichern. 📄 🗨

<https://www.heise.de/newsticker/meldung/avm-entweicht-geheimer-fritzbox-schluesel-3448752.html>

ct Fotografie
Aus der c't Fotografie-Galerie
Fotografen vorgestellt



Heute: Die Bilder der c't-Foto-Galeriefotografen 'Pietmaedchen'

Top-Newsletter
Die wichtigsten
Nachrichten
2 x wöchentlich.

[heise online](#)

SRC: <https://www.heise.de> (11.11.2016)



FRITZ!Box Keyble

Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

- AVM ships private key for Euro-DOCSIS-signed intermediate CA on Router.
- On-the-fly generation of VALID modem certificates.
- Presumably trusted by many CMTS around the world (Trusting the Euro-DOCSIS Root-CA)



FRITZ!Box Keyble

Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

10.11.2016

Certificate exchange for cable routers

In the course of a certificate exchange, AVM has been using new and improved manufacturer certificates since 2015. Older certificates were exchanged by software updates from cable providers. Users don't have to do anything. Misuse of older certificates was not reported.

1

- German ISPs and AVM working on updating old devices and blocking compromised CA in their CMTS.
- What about the rest of the (Euro)-DOCSIS world?

¹<https://en.avm.de/service/current-security-notifications/>

Hacking DOCSIS

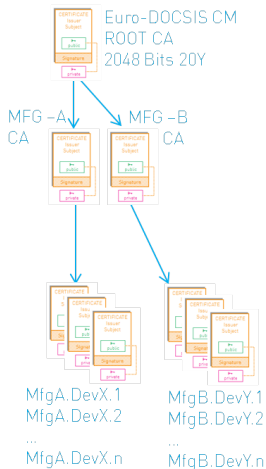
Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"



SRC: <https://www.excentis.com/blog/certificates-and-different-pkis-docsis-31>



Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

Listing 1: AVM Cable Modem Root CA

```
Certificate:  
  Data:  
    Version: 3 (0x2)  
    Serial Number:  
      18:d9:3d:04:72:8f:ce:2f:ba:a7:81:a8:1f:92:6a:43  
    Signature Algorithm: sha1WithRSAEncryption  
    Issuer: C=BE, O=tComLabs - Euro-DOCSIS, OU=Cable  
      Modems, CN=Euro-DOCSIS Cable Modem Root CA  
    Validity  
      Not Before: Jul 30 00:00:00 2009 GMT  
      Not After : Jul 29 23:59:59 2029 GMT  
    Subject: C=DE, ST=Berlin, L=Berlin, O=AVM GmbH, OU=  
      Euro-DOCSIS, OU=Germany, CN=AVM GmbH Cable  
      Modem Root Certificate Authority
```



"Revocation"

Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

"My CMTS is not using that certificate, am I safe now?"

No, because (Euro)DOCSIS is designed to accept any correctly signed cable modem by default, the certificate might be used by a hacked modem in the future without you noticing it. Hence, it is important to configure ALL your CMTSs not to accept the revoked certificate anymore!"²

²<https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates/revoked-certificates>



"Revocation"

Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

"Two centralized methods are defined in the specifications (CRL and OCSP). None of these are required to be supported. No public CRL or OCSP service for (Euro)DOCSIS exists."³

³<https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates/revoked-certificates>



"Revocation"

Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

```
# snmpset -v 2c -c <community> <cmts_ip>
docsBpi2CmtsCACertStatus.<index> i 4 docsBpi2CmtsCACertTrust.<index> i 2
docsBpi2CmtsCACert.<index> x <hexString>4
```

⁴<https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates/revoked-certificates>



"Revocation"

Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

Euro-DOCSIS PKI

AVM Intermediate CA

"Revocation"

33c3@joel-stein.de