p1b26i1294s0-.pdf

Unknown

From: Conus Joël
Sent: Tuesday, October 15, 2002 3:10 PM
To: Alan (E-mail); Bongard Dominique; Chnstophe Nicolas; Groux Cédric, JJ Gee (E-mail); Kudelski Henri; Sasselli Marco; Valsecchi Patrick
Subject: [DTV]

Attachments: DTV 20021015.txt.asc

DTV 20021015.txt
(10 KB)

```
*** PGP SIGNATURE VERIFICATION ***
*** Status:   Good Signature
*** Signer:   Joël Conus <conus@Nagra.com> (0xACC187D8)
*** Signed:   10/15/2002 3:07:15 PM
*** Verified: 6/5/2007 11:06:57 PM
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***

The CAM ID / ZKT pair posted on a forum yesterday doesn't come from a P4 card. While the
CAM ID is in the P4 range, it doesn't pass all the ZKT challenges. Over time, the
receiver will send various challenges to the card and if a challenge yields a wrong
answer, the IRD will display an "EXT 745" error.
Some people are working on building ZKT tables and they are trying to find partially
matching CAM ID's using a brute force method. As long as the receiver doesn't try a non-
working challenge, the card loaded with this information will keep on working fine and
if its CAM ID is in the P4 range the IRD will think it is "talking" to a P4 card.


*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```


CASE NO.
SA CV 03-950 DOC (JTLx)
ECHOSTAR SATELLITE CORP., et al.,

vs.

NDS GROUP PLC, et al.

DEFENDANT'S EXHIBIT 1234

DATE _____ IDEN.

DATE _____ EVID.

BY _____
Deputy Clerk

p1b26i1294s0-.pdf

Unknown

From: Conus Joël
Sent: Tuesday, October 15, 2002 3 10 PM
To: Alan (E-mail); Bongard Dominique; Christophe Nicolas, Groux Cédric, JJ Gee (E-mail); Kudelski Henri; Sasselli Marco; Valsecchi Patrick
Subject: [DTV]

Attachments: DTV 20021015.txt.asc

DTV 20021015.txt
(10 KB)

```
*** PGP SIGNATURE VERIFICATION ***
*** Status:    Good Signature
*** Signer:    Joël Conus <conus@Nagra.com> (0xACC187D8)
*** Signed:    10/15/2002 3:07:15 PM
*** Verified: 6/5/2007 11:06:57 PM
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***

The CAM ID / ZKT pair posted on a forum yesterday doesn't come from a P4 card. While the
CAM ID is in the P4 range, it doesn't pass all the ZKT challenges. Over time, the
receiver will send various challenges to the card and if a challenge yields a wrong
answer, the IRD will display an "EXT 745" error.
Some people are working on building ZKT tables and they are trying to find partially
matching CAM ID's using a brute force method. As long as the receiver doesn't try a non-
working challenge, the card loaded with this information will keep on working fine and
if its CAM ID is in the P4 range the IRD will think it is "talking" to a P4 card.


*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```