Marketing Competitive Intelligence

NDS and Nagra Conditional Access Systems

A Technical and Business Analysis

Classification:	**Confidential**
Restricted to:	**NDS Employees Only**

Doc. Designation	MQ-R084
Release:	A
Date:	May 13, 2001
Owner:	Steven Grossman
Writer:	Steven Grossman, Helith Sofer

All information contained in or disclosed by this document is considered confidential and proprietary by NDS Ltd. NDS Ltd. reserves the right to use this design in other projects without reference to the recipient. By accepting this material, the recipient agrees that this material and the information contained therein will be held in confidence and in trust and will not be copied or disclosed in whole or in part to any third party

The reproduction of any trademark or service mark, registered or otherwise, belonging to any third party appears here for the purposes of identification of the goods or services of that third party only Such reproduction is at all tim accordance with honest practices

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

vs.

NDS GROUP PLC, et al.

DEFENDANT'S EXHIBIT 1270

DATE ________________ IDEN.

DATE ________________ EVID.

BY ______________________
Deputy Clerk

NDS

Marketing Competitive Intelligence

NDS and Nagra Conditional Access Systems

A Technical and Business Analysis

Classification:	**Confidential**
Restricted to:	**NDS Employees Only**

Doc. Designation.	MQ-R084
Release:	A
Date:	May 13, 2001
Owner:	Steven Grossman
Writer·	Steven Grossman, Helith Sofer

NDS and Nagra Conditional Access Systems
A Technical and Business Analysis

Table of Contents

1. Scope

This document is a highly confidential report specially prepared by NDS Marketing Competitive Intelligence for its Worldwide Sales and Marketing Staff. It contains a comparison between the conditional access systems of NDS (VideoGuard) and Nagra (NagraVision).

Please respect the confidentiality of this document as it makes use of information sources proprietary to NDS. While we encourage readers to utilize this information as required during the course of business, copies of this document are not intended for distribution outside of NDS.

The intent of this analysis is to directly address a variety of key business and technology issues that NDS staff may confront when meeting with customers. It is hoped that the document will be used as ready-reference material.

Audience

This analysis will be of benefit for several audiences with varying requirements and levels of technical orientation.

a. Worldwide NDS Marketing and Sales Staff when facing Nagra as a competitor. The analysis provides ready answers to a number of business and technical issues they may confront.

b. Management and Executive Staff who require a top-line overview of key issues and comparisons between NDS and Nagra.

Format of Analysis

This analysis has been organized into four major topic areas. These areas include discussions of overall business reliability, a systems comparison, business enabling features and ability to combat piracy. Specific issues are brought out and elaborated upon in each area, highlighting the differences between NDS and Nagra. To improve readability, the NDS response to each issue is printed in ***bold italics.***

Important Note

Information contained in this document, particularly technical data, is derived from a variety of sources, both proprietary and within the public domain. NDS Marketing Competitive Intelligence believes this information to be accurate as of the date of publication. We continually update our knowledge base about Nagra and other major competitors and will immediately inform NDS staff concerning significant changes in Nagra's technology, business applications or business strategies. We encourage readers to get back to us with your questions, comments or suggestions.

2. Doing Business with a Reliable Company

NDS reliably develops and implements digital broadcast systems throughout the world and continually invests in new cutting-edge technology.

2.1. NAGRA SUBSCRIBER NUMBERS ARE INFLATED

Nagra claims to have over 19 million digital TV subscribers. This is not the case.

Nagra counts as subscribers all cards that were ever shipped to their customers, including those not yet activated, discontinued subscribers and replacement cards to existing or former (analog broadcasters that have ceased operations) subscribers. Such an approach leads to greatly inflated subscriber counts.

Comparably, NDS has shipped 49 million digital smart cards, two and one-half times that of Nagra.

NDS maintains a count of over 22 million documented active digital subscribers. Our internal analysis reveals that Nagra has fewer than 9 million documented active digital subscribers, less than half of NDS.

NOTE: If you wish to view a more in-depth analysis of the NDS vs Nagra subscriber count, please refer to the MarketScope: Counting Digital TV Subscribers - NDS vs Nagra (25 April, 2001). A copy is available from Steve Grossman.

2.2. NAGRA DELIVERS LATE!

According to an inside source, Nagra has "many new customers but cannot deliver."

Nagra stopped delivery of conditional access modules (CAMs) to TV Cabo, the Portugal Telecom multichannel operator for a two month period in Fall, 2000. It is not known if delivery has been resumed. The interruption was due to a lack of component availability at Nagra. TV Cabo has around 800,000 subscribers, of which 100,000 are DTH subs with Nagra conditional access set-top boxes (See Appendix D).

NDS has been praised by its customers, such as Tevel in Israel, in a public press release (See Appendix E) for delivering a full cable system with advanced features in the short time period of three months.

2.3. LOW R&D INVESTMENT

Nagra only invests about 20% of revenues in R&D activities (See Appendix A). Nagra relies heavily on partner relationships to supply innovative services.

NDS invests heavily into R&D to ensure that its conditional access systems are by far the most technologically advanced. NDS is also committed to supplying the most savvy technology ensuring that customers retain their leading market share.

NDS is pioneering developments in interactive television, XTV and datacasting – the streaming media solution for DTH companies.

NDS is now investing in digital rights management to ensure that the TV operator is able to protect highly valuable content while stored on a personal computer.

3. Systems Comparison

NDS is committed to continually improving its conditional access systems and achieves unprecedented security with its unique smart card technologies.

3.1. SMART CARD TECHNOLOGY

"Off-the-Shelf" Chip Technology

Nagra smart cards rely on "off-the-shelf" chip technology. Nagra's chip suppliers offer the same product to many different customers (their chip is used by Irdeto and Canal+ as well). As such vulnerabilities in the hardware platform will eventually be felt by all of Nagra's customers. Security problems discovered in applications using these off-the-shelf chips can, and have been used against Nagra's smart cards. Additionally, Nagra does not customize smart card platforms for every customer but instead provides each one with a different software version.

Chip Technology Implication: the "Domino Effect"

Nagra's approach exposes customers to a "domino effect" in which the hack of one system compromises other customers to pirate attacks, increasing customer risk. For example, once EchoStar in the U.S. was hacked, the Via Digital (Spain) and ExpressVu (Canada) systems were subsequently pirated. Technical details and development tools are freely available on the Internet to assist hackers and they share this technology from one Nagra customer to the other. NDS now sees that pirates are recycling Nagra hacks into other parts of the world, notably China and the Pacific Rim.

Nagra hacks are readily available at the following sites:

Iceman E3M Website - ***http://members.home.net/tsmallbridge/index.htm***
(EchoStar – US)

Dishnethack.net - ***http://www.dishnethack.net*** (EchoStar and ExpressVu – Canada)

Zacky Files – ***http://www.geocities.com/zackyfiles/*** (Via Digital – Spain)

Because of legal issues, these web sites may be closed down from time to time. Please take caution prior to forwarding these sites to customers since they may contain information concerning the DIRECTV hack. For the most up-to-date information contact Steve Grossman.

NDS developed its own proprietary technology for its smart card and each NDS customer receives its own unique smart card platform. Because NDS uses unique algorithms for each customer, customer risk is minimized. Unlike Nagra, if an NDS system is hacked, the hack will not effect other systems.

For example, although DIRECTV was hacked, it had no effect on the security of other NDS customers. As proof, the digital BSkyB system has been operational since October 1998 and has not been hacked.

3.2 INFERIOR ENCRYPTION TECHNOLOGY

Nagra's key-based encryption technology is inferior to NDS's algorithm-based approach. Below are some major points highlighting how NDS overcomes many of the deficiencies inherent in Nagra's system.

- Nagra's key-based system generates the control word – used to encrypt and decrypt the transport stream - directly from the Entitlement Control Message (ECM). Protecting the system requires regular key updates, necessitating the transmission of secret information between the headend and the subscriber's smart card.

- ***NDS's algorithm-based VideoGuard system uses proprietary algorithms to generate control words. VideoGuard does not require transmission of secret information between the headend and the subscriber's smart card. All secret/encrypted information remains on the smart card.***

- Nagra's key-based system uses fixed, usually known algorithms such as DES to protect the control words When a key-based system is pirated, the keys used by these algorithms must be updated, but the algorithm remains the same. Therefore, once hacked, the algorithm can be used over and over again.

- ***If an NDS system is compromised, the algorithm itself is changed with no need for key updates. With NDS's algorithm-based system, many more of the CA system components – including the algorithms themselves – are "subject to change without notice." NDS introduces more uncertainty into the hacker's world since the security employed remains a "moving target."***

- Nagra's key-based system requires lots of bandwidth to update keys and TV operators need to manage a complex key database. This is time-consuming and costly to the TV operator.

- ***NDS's system utilizes minimal bandwidth when sending secured information such as Entitlement Management Messages (EMMs) to subscribers. NDS internal analysis reveals that VideoGuard utilizes up to 90% less bandwidth than Nagra for such operations. For large TV operators with millions of subscribers, NDS estimates this extra bandwidth can result in several million dollars of additional costs annually to the TV operator.***

For a more in-depth technical discussion of key-based versus algorithm-based encryption systems, please refer to NDS document WP-R029 "Why NDS Uses Algorithm Based Security" by Yossi Tsuria and Stephanie Wald.

3.3 LONG SUBSCRIPTION RENEWAL CYCLES

Nagra's automatic subscriber renewals take up to 12 hours for every half-million subscribers. This is due to poor bandwidth utilization because of Nagra's key-based encryption method.

NDS's algorithm-based security utilizes minimal bandwidth – therefore renewals are carried out more quickly and efficiently. Renewals are carried out in 20 seconds instead of hours. This capability saves the TV operator time and money.

4. Business Enabling Features

4.1. EXPENSIVE SHRINK-WRAPPED APPROACH

Nagra relies on a packaged, "shrink-wrapped" approach with essentially the same system being sold to all customers.

Nagra's typical bid includes costs for computer hardware and software licenses for a basic system (≈50,000-100,000 subscriber capacity). To scale up to meet increased business needs (even to 250,000 subs) a customer must "buy" additional capacity from Nagra. As well as new licenses, prices for Nagra upgrades include additional system integration and additional engineering consultation that can run up to $1,500 per person per day!

With NDS you know exactly what you are getting. NDS personalizes the system together with its customers for an end-to-end customized solution. This ensures that the full system is known in advance and designed to be "future-proof" for any additional application or service that the TV operator wishes to include with future upgrades.

4.2. ADDITIONAL COSTS FOR ADVANCED FEATURES

Nagra offers features such as OPPV, IPPV and NVOD as optional add-ons to their conditional access package at an extra price.

For example, adding IPPV to Nagra's basic CA package requires purchasing their Call-Collector system and the necessary integration and engineering support. Our estimates indicate that Nagra's Call Collector system can add **up to US $150,000** over the basic system configuration!

NDS offers OPPV, IPPV and NVOD as standard conditional access features.

NDS's VideoGuard provides a feature-rich, flexible and easy-to-use environment that allows TV operators to operate their OPPV, IPPV and NVOD business in a manner that will allow additional viewer revenue.

See Appendix C for additional feature comparisons.

4.3. EPG: HARD TO INTEGRATE AND MANAGE

Nagra needs to integrate separately with each EPG on each STB.

When a customer chooses Nagra's conditional access system, each STB manufacturer must create its own independent solutions for STB-related features such as channel tuning, STB setup, OSD (on-screen display), parental control and email features. Each is controlled separately from the headend and each STB needs its own instructions to the hotline for support of the customers.

NDS, through its integrated EPG and conditional access system, allows the TV operator's headend to control all STBs from any supported manufacturer simultaneously. The TV operator's hotline deals with everyone as having the same interfaces no matter which of the STBs they are using. Software development for applications such as interactive television is done once and works the same on all STBs.

4.4. END-TO-END INTEGRATION: NOT THEIR OWN RESPONSIBILITY

Nagra cannot offer its own end-to-end integration.

Nagra partners with other groups such as EchoStar who have their own agenda and interests. There is never a clear definition of responsibility for integration.

NDS assumes full responsibility for end-to-end integration when requested to do so and has done this integration at a number of sites, both for News Corp and non-News Corp customers.

4.5. POOR BLACKOUT CONTROL

Nagra utilizes the Subscriber Management System (SMS) to initiate blackouts – releasing full control of this function from the conditional access system.

Nagra provides blackouts through the Entitlement Management Message (EMM) generated from the SMS. The information is held in the subscriber system and not the content. If you filter out a Nagra EMM, you can overcome blackouts, potentially cutting into the TV operator's profits and with the threat of placing the operator in legal jeopardy with local sports content providers.

NDS sets blackout assignments via global EMMs in combination with the Entitlement Control Message (ECM), thereby ensuring that the content is kept even more secure. NDS provides an extra level of blackout security. This enables NDS customers such as DIRECTV to securely offer "premium" sports packages and generate additional revenue streams.

5. Combating Piracy

Combating piracy is a proactive policy at NDS. NDS engages vigorous electronic countermeasures against pirate devices and does not accept piracy as "a fact of life."

5.1. POOR COUNTERATTACK

Nagra is not capable of successfully launching an electronic countermeasure to fight a hack.

In the United States, pirates have found Nagra's electronic countermeasures (ECMs) ***easy to overcome.*** Hackers are always aware of Nagra's attempts a day prior to a Nagra counterattack due to the length of time it takes them to actually broadcast the attack. This gives the hackers the chance to defend their illegal viewers.

In some cases, such as Via Digital in Spain, the installed Nagra CA system ***doesn't even support ECM functionality at all.***

NDS has years of proven experience in successfully recovering from hacks via ECMs. Our customers use our unique electronic countermeasures to knock out illegal viewers right before key events.

As of the end of January 2001 both EchoStar (Nagra) and DIRECTV (NDS) in the United States were hacked. NDS successfully countered a DIRECTV pirate attempt in the US on what is being called "Black Sunday" by the hacker community. NDS's countermeasures were sent right before the SuperBowl. According to external literature, over 200,000 pirate devices were disabled. NDS field contacts confirmed that Nagra did not start sending an ECM until after the game was over. Anyone with a pirated Nagra card saw the game for free. Our estimate is that this commercial loss to EchoStar probably accounted for over 100,000 non-paying subscribers.

5.2. WEAK OPERATIONAL SECURITY

From our observations of Nagra's activities in the field, they have an extremely weak ongoing operational security function.

Instead of a field team, Nagra only relies on ongoing software upgrades to combat piracy since their key downloads are exposed to hacking.

NDS maintains an operational security team of 20 people worldwide with background and experience in intelligence, and specializing in battling piracy. This means that NDS is well-positioned to thwart hacking or, at the

very least, delay it, thereby minimizing or totally eliminating a customer's financial loss.

NDS's service is regarded as unique — even to the point that other companies come to us for consultation.

Appendix A: General Comparison

	NDS (VideoGuard)	Kudelski (NagraVision)
Headquarters	UK	Switzerland
Ownership	Public – NASDAQ Investors: NewsCorp (80%)/Free Float (20%)	Public – Swiss Exchange (SWX) Investors: Kudelski Family (37%)/Free Float – mostly US and UK (53%)/Dassault Group (10%)
# of digital conditional access technology customers worldwide	Over 22M[1]	≈9M[2]
% of revenues invested in R&D	30%[3]	15-25%[4]
# Employees	Over 1,000	425[5] (there are rumors of significant cutbacks to approximately 300, however)

[1] Source: NDS

[2] Source: NDS internal report entitled "Nagra Subscribers"

[3] Source Dresdner, Kleinwort, Wasserstein Research (DKWR) Interactive TV Software" – 26 January, 2001

[4] Source Dresdner, Kleinwort, Wasserstein Research (DKWR) Interactive TV Software" – 26 January, 2001

[5] Source: Kudelski Web site – "Key Figures"

Appendix B: Technology Comparisons

B.1. CARD TECHNOLOGIES

	VideoGuard	NagraVision
Platform	Multiple, proprietary, unique smart card chip design for each customer	Off-the-shelf
Memory Size	16kROM, 8kEEPROM	16kROM, 4kEEPROM
Securily System	Algonthm-based	Key-based
Encryption	Fast proprietary algonthms	Public keys
Card authentication	Yes – NDS propnetary "Fiat-Shamir" authentication scheme	No
Automatic subscriber renewals	20 seconds per 500,000 subs	12 hours per 500,000 subs
Headend Security	Server is designed to be more secure than a smart card	ECE and EME which handle encryption contain a "mother smart card." The mother smart card controls the securlty of the ECE and EME

B.2. STB TECHNOLOGIES

	VideoGuard	NagraVision
STB supporting mail/OSD	Yes	No*
EPG support	Integrated part of the CA	Based on 3rd party EPG provider
Secure software download over air	Available	No**

*The STB can do this but it is not on the EPG and differs for each type STB in the field

**The STB can do this but it is then not in the control of the headend and is different for each type STB in the field

Appendix C: Business Enabling Features

	VideoGuard	NagraVision
Logical group addressing for entitlements	Yes	No
Logical group addressing for pricing	Yes	No
Parental control	Yes	No*
Moral rating	Yes	No*
Smart card supports spending limits	Yes	No
Viewing history	Yes	No
Personal email	Yes	No*
General email	Yes	No*
Group-directed email	Yes	No*
Email save/delete features	Yes	No*
Electronic Billing	Yes	No
Content secured blackout and spot features	Yes	Yes**

* relies on STB

** content security does not incorporate blackout and spot features

Appendix D: *Inside Digital TV* Brief

"BRIEFLY" ***From INSIDE DIGITAL TV*****, October 30th, 2000**

The supply of Nagra conditional acccss modules (CAMs) to TV Cabo, the Portugal Telecom multichannel operator, was interrupted two months ago and has not been resumed since. The CAMs are distributed by two exclusive importers.

A spokeswoman for one of them was unable to give a date for resumption of the deliveries and said that the interruption was due to a lack of components to manufacturer Kudelski in Switzerland. TV Cabo has around 800,000 subscribers, of which 100,000 are DTH subs with Nagra CA set-top boxes.

Appendix E: *Business Wire*

Tevel Digital Chooses NDS as Its Digital Cable TV Technology Partner - *Business Wire: Thursday, August 17, 2000*

LONDON--(BUSINESS WIRE) via NewsEdge Corporation -- NDS Group plc (NASDAQ/EASDAQ: NNDS), a News Corporation (NYSE: NWS) company, and a leader in providing business solutions to content owners and TV channels through sophisticated interactive TV technology, has been chosen by Tevel - Israel International Communications Ltd -- a leading cable TV operator in Israel, to provide NDS Open VideoGuard(TM) digital conditional access, NDS StreamServer(TM) broadcast management systems and to be the system integrator for Tevel's move from analog to digital broadcasting. NDS has also been awarded a service contract to ensure that Tevel's digital service remains on-air and fault-free.

"I am pleased to be able to announce Tevel as NDS' latest digital cable contract win. As well as providing the TV industry's most widely used conditional access system, Open VideoGuard, NDS has also provided the interactive software systems for many of the industry's leading and most powerful interactive applications to date. This experience means that NDS is one of the few companies that has the knowledge and expertise to guide analog broadcasters and operators towards the profitable provision of secure new digital services," says Dr. Abe Peled, President and CEO of NDS Group plc.

"I believe that it is this digital leadership which led to Tevel choosing us as digital technology partners. I am equally sure that other analog cable operators will come to the same conclusion as they search for the right organization to assist their move to digital distribution," added Peled

The Tevel digital service aims to be on-air by the end of August 2000 and will run in parallel with Tevel's analog service. Presently Tevel is a leading cable operator in Israel, with its services being received by 440,000 households.

"We know that by working with NDS we have a partner that has the right digital technologies, and has unrivalled experience and understanding of the TV business to ensure that our new digital service has the greatest chance of success," says Yossi Douer, Managing Director of Tevel. "With NDS' help, we look forward to converting our analog customers to digital and winning new customers by offering our advanced innovative and easy to use new digital 'Tomorrow's World' interactive TV services."

About Tevel

Tevel Israel International Communications Ltd. was established in 1988 to develop, construct and operate cable television systems in Israel. Tevel's five franchises, including the entire Tel Aviv-Givatayim metropolitan area, have an overall potential of about 660,000 homes (40% of Israel's homes). Tevel has completed network construction in all five areas and has about 430,000 subscribers. In November 1999, Tevel acquired 35% of Golden Channels, which has around 340,000 subscribers in the areas of Jerusalem, Ramat Gan, Beer Sheva, Acco, and Nahariya. The acquisition is yet to be approved by the Antitrust Authority and the CATV Council.