

RECEIVED

DEC 22 1992

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

ORIGINAL
FILE

Before the
F E D E R A L C O M M U N I C A T I O N S
C O M M I S S I O N
Washington, D.C. 20554

In the Matter of)
)
)
)
Inquiry into Encryption Technology)
for Satellite Cable Programming)

PP Docket No. 92-234

C O M M E N T S O F
DECTEC INTERNATIONAL INCORPORATED

John Grayson,
Chief Executive Officer
DECTEC International Inc.

DECTEC International Inc,
P.O. Box 2275,
1962 Mills Road,
Sidney, British Columbia,
Canada. Postal Code: V8L 3S8
Telephone (604) 655-4463
Facsimile: (604) 655-3865

Dated: December 20, 1992

No. of Copies rec'd 5 copies
List A B C D E

TABLE OF CONTENTS

SUMMARY.....	1
I. INTRODUCTION.....	2
II. STANDARD DECODER INTERFACE.....	5
III. COMPETITION IN THE PROVISION OF VC II COMPATIBLE DECODER MODULES.....	6
IV. ACCESS TO THE DBS AUTHORIZATION CENTER.....	7
V. SECURITY OF THE VC II SYSTEM.....	10
VI. THE PRICE OF A CONSUMER DECODER.....	11
VII. CONCLUSION.....	12

SUMMARY

After a short introduction, DECTEC will comment on and support the establishment of a Standard Decoder Interface; that competition be encouraged in the supply of VC II compatible decoder modules; review the benefits of access to a common DBS Authorization Center; comment on the security problem which commercial VC II decoders pose; and conclude with a recommendation of a fair price for a consumer decoder sold in an openly competitive environment.

I. INTRODUCTION:

DECTEC International Inc. is a privately held Canadian company. Since 1986, DECTEC has been active in Research and Development in the field of Encryption Technology.

In 1990, DECTEC announced the development of a new approach to Encryption Technology for Satellite Cable Programming. This new approach will now be briefly explained.

Traditionally, a piece of electronic equipment is divided into two sections: 1) Hardware and 2) Software. The HARDWARE portion is typically represented by the physical components: the circuit board, the components, the case. The SOFTWARE is typically a computer program or series of small computer programs which reside in the memory of one or more of the electronic components on the circuit board. These computer programs typically provide primitive control commands for the proper operation of the Hardware.

What DECTEC changed in it's new approach to Encryption Technology was to eliminate the concept of application specific Hardware. In other words, DECTEC demonstrated that

it was no longer necessary to build a separate and unique circuit board for every type of different Encryption Technology.

DECTEC replaced what was heretofore application specific hardware with a neutral digital hardware platform. This meant that a circuit board containing hundreds of thousands of empty digital gates could be configured or reconfigured by SOFTWARE to instantly become virtually any type of HARDWARE.

In the area of Encryption Technology, this approach can provide great savings to the consumer. For example, this design approach would allow a consumer to buy one decoder box, but be able to purchase programming which utilized a variety of Encryption Technology systems. All of these systems would be described in software and stored in a reprogrammable "smart card". As the consumer switched from channel to channel and changed from one Encryption Technology to another, the decoder box would instantly change the hardware functions to match the Encryption Technology in use. At the present time a consumer must buy a separate decoder box in order to gain access to each different Encryption

Technology. Whereas with the DECTEC approach, the consumer would only have to buy one decoder box. Refer to Exhibit A for further details.

This approach was largely developed to address a particular Canadian problem in Encryption Technology: the coexistence of TWO Encryption Technologies transmitting two different types of scrambled signals to Canadian consumers. The problem which faced CANCOM, one of the Canadian signal suppliers, was that Canadian consumers could not afford the price of two decoders. The DECTEC design solved this problem.

It is interesting to note that this design is solely based on North American technology. Every major component used in the DECTEC design is manufactured in the United States.

It is not difficult to see that this "all in one box" design would threaten the very foundation of incumbent suppliers of Encryption Technology. These suppliers were and still are committed to selling the consumer a separate decoder box for each Encryption Technology used. See Exhibit B.

Conversely, a DECTEC decoder can also be configured to be just a simple, secure, VC II compatible device. Viewed from this perspective, the implementation of a Standard Decoder Interface referenced in this Inquiry, makes good sense.

II STANDARD DECODER INTERFACE:

DECTEC is in full support of an FCC mandated Standard Decoder Interface. Here are our reasons:

- 1) Substantial benefit to the consumer through:
 - a) lower decoder prices
 - b) ease of consumer operation
- 2) Substantial benefit to the American manufacturer through:
 - a) elimination of redundant and duplicated circuits
 - b) a stable equipment design standard
- 3) Substantial benefit to the American Programmer through:
 - a) removal of dependency on a single Encryption supplier
 - b) cost savings through competition between Encryption suppliers
 - c) the ability to easily switch encryption systems should any particular encryption supplier fail to maintain the security of their encryption system
- 4) Substantial benefit to the Encryption Supplier through:
 - a) significantly lower manufacturing costs
 - b) the ability to develop substantially smaller consumer decoder modules
 - c) the ability to innovate new design features which would benefit the American consumer
 - d) the ability to develop a decoder product which could be sold to international markets

For these reasons, we urge the FCC to establish a Standard Decoder Interface port which is no greater than 2.5 inches in length whereby at least six (6) Standard Decoder Interface ports could be placed on the back of any typical consumer or commercial television receiving equipment. The current de facto interface standard would be acceptable to DECTEC.

III COMPETITION IN THE PROVISION OF VCII COMPATIBLE DECODER MODULES:

DECTEC supports the concept of competition in the provision of VCII compatible decoder modules.

Since DECTEC has already designed it's own decoder module which can secure and decode VC II system signals in it's own unique proprietary way, DECTEC's interest in competing is obvious.

It should be noted that DECTEC's emulation of the VC II system does not make use of any processes proprietary to either Titan Linkabit or General Instrument. See Exhibit C.

IV ACCESS TO THE DBS AUTHORIZATION CENTER:

Following years of Research and Development and one year of extensive discussions with U.S. programmers, DECTEC concluded that it did not make good business sense to market a competing decoder in the United States as long as General Instrument maintained control over the DBS Authorization Center.

The programmers were not interested in having a multiplicity of DBS Authorization Centers to authorize their subscribers through. See Exhibit D for comments from programmers.

DECTEC wrote to the President of General Instrument on two separate occasions to request access to the DBS Authorization Center for the purpose of addressing DECTEC designed, VC II compatible consumer decoder modules. DECTEC's most recent request was refused without discussion. See Exhibit E.

Following our discussions with programmers, DECTEC concluded that as long as General Instrument maintained administrative and technical control of the DBS Authorization Center, programmers would not be in a position to even test alternative and competing systems.

DECTEC urges the FCC to encourage General Instrument to relinquish administrative and technical control of the DBS Authorization Center to a neutral and not-for-profit entity.

This NEUTRAL ENTITY would be responsible for:

- a) day to day administration of the Center
- b) technical control of all data
- c) establishing competing decoder addressing standards
- d) protecting the confidentiality of each programmer's list of customers
- e) ensuring the security of all subscriber authorization codes

DECTEC anticipates that General Instrument will object to such a proposal, claiming proprietary interests in the current DBS Authorization Center. Legal research indicates that any such interests are either unsubstantiated or unpublished.

In consideration of General Instrument's likely position, two options are available.

First, it is the practise in the computer industry to pay a license fee for the use of system level computer programs such as Bios and DOS. An independent tribunal of intellectual

property experts could be appointed by the FCC to review General Instrument's claims of proprietary interest in the DBS Authorization Center. If the claims are substantiated, the tribunal would assess a one time license fee per subscriber to be paid to General Instrument by each competing Encryption Technology user.

Second, if the foregoing suggestion proves to be unworkable, the current DBS Authorization Center could be phased out and replaced with an independently designed and operated Authorization facility. However, DECTEC recommends that the establishment of a new Authorization Center not be sanctioned by the FCC unless it's facilities were to be made available on a not-for-profit basis to any competing technology.

In 1991, with the financial support of the National Research Council, Government of Canada, DECTEC designed and built it's own DBS Authorization System. DECTEC's Authorization System has ten times greater capacity than the DBS Authorization Center presently used by General Instrument. See Exhibit F.

It is our understanding that Titan Linkabit has, as well, designed a DBS Authorization Center.

V SECURITY OF THE VC II SYSTEM:

DECTEC has two comments to make in this respect.

First, DECTEC agrees with the FCC assessment in this Notice of Inquiry, that the "flaw has been in the conditional access portion of the technology rather than in the encryption algorithm itself."

To demonstrate this fact, DECTEC met with officials from Reiss Media in 1989, a major pay-per-view programmer. DECTEC proposed a simple pilot project to demonstrate that commercial VC II's could be secured by installing what is now known as a "smart card" in each commercial VC II. However, since the pilot project required minimal cooperation from the DBS Authorization Center, the proposal was not acted upon. See Exhibit G.

Secondly, in response to the request for comments "on the implications for the security of the GIC system of retaining the commercial VC II units." DECTEC's position is very clear. The VC II system cannot be fully secured for competitive use as long as non secure commercial VC II units are left operating in the field. These units must be replaced or secured by other means. No manufacturer of any type of secure decoder can compete against the continued presence of pirated commercial VC II's.

VI THE PRICE OF A CONSUMER DECODER:

We agree with the current President of General Instrument when he stated before the U.S. House of Representatives on March 6, 1986: "The module, when it is incorporated into HTVRO receivers, should result in a price increase of only about \$175 over receivers without a module. If competitive second-source manufacturers are more adept with high volume manufacturing of the modules than M/A-COM, the price may go even lower." See Exhibit H.

One hundred and Seventy Five dollars per decoder module is a very profitable figure when one considers the actual manufacturing cost. A price higher than \$175 for a single purpose consumer decoder, in our view, would be both unwarranted and excessive. In a competitive environment, the price could move even lower. Please refer to the Cost Comparison charts on pages 16, 17, and 18 of Exhibit I.

VII CONCLUSION:

DECTEC supports the concept of competition at all levels in field of Encryption Technology.

On January 31, 1992, Senator Gore made an inspiring and dramatic late night speech before the Senate concerning Bill S-12. See Exhibit J for the complete text. I quote here just two short paragraphs from page S738 of the Congressional Record - Senate.

"I quote a letter from Mr. Charles Hewitt, president of SBCA, who states: The precept of program access "is very basic: Let competing technologies get to the 'starting line' with as few impediments as possible. After that, television viewing households can decide which means of video distribution will best serve their needs, and the marketplace will take care of the rest."

"It could not be better said: Let competition exist and consumers will choose. That is the American way, the way embodied in this Legislation."

NEWS NEWS NEWS

NEWS NEWS NEWS

For Immediate Release



DECTEC International Inc.

PO Box 2275, 1962 Mills Road

Sidney, British Columbia

V8L 3S8, Canada

Tele: (604)655-4463 Fax: (604)655-3865

September 2, 1991

**DECTEC LAUNCHES MARKETING CAMPAIGN:
SHIPS S.U.N. DECODER IN CANADA; UPSETS GI MONOPOLY**

DECTEC International Inc. began shipping its Secure Universal Norm descramblers on Friday, August 30 to distributors across Canada.

Following discussions with customers during both the Nashville and Calgary trade shows and after two months of one-on-one meetings with distributors throughout Canada, DECTEC has positioned its S.U.N.[™] decoder to compete head-to-head with General Instrument's VCII Plus[™]. Over the past two days, DECTEC has already written orders for just under 1,000 units, and the company has shipped several hundred S.U.N. decoders into the field.

"We're thrilled that we were able to put our product into the market before the start of the busy fall season," remarks John Grayson, CEO of DECTEC International Inc. "We've tested the final rewrite of the S.U.N. software and we're anticipating an exciting first couple of months."

Canadian distributors are excited about the S.U.N. product. "Our distributors like having a choice," explains Colin Ewart, Director of New Business Development at DECTEC. "We can offer a better technology at a lower price. It's what competition is all about."



Recycled Paper

"Our biggest concern," Mr Grayson says, "is selling against pirate VCIIs. In a secure environment, we project first year sales in Canada at 20,000 units or 40% of the new dish market. However, if what our distributors report is correct and GI continues to recondition and recycle old VCII's for pirate applications in Canada, our share will drop to maybe 5% or 10%, making our projections incorrect."

DECTEC will launch a "KEEP THE FACTS STRAIGHT" advertising campaign throughout Canada to counter slander and disinformation circulated by GI and GI's two biggest Canadian distributors, Satellite Supply and Channel One. "We expect the next few months will get a bit toasty," says Mr Ewart. "GI's not going to like the fact that we're selling a better product at a lower price. But distributors have already seen the benefits. Since our pre-launch announcement, GI has told distributors, here, that they would drop the price of the Plus. We think our distributors will stay with us even if GI lowers its price and reverts to name calling."

S.U.N. descramblers are shipped authorization-ready. Only non-subscription services presented in the clear are viewable without authorization and payment.

"As a company we have spoken to every major and almost every single basic programmer," explains Mr Grayson. "Nearly everyone we've sat down with is interested in what we have to say, and we sincerely appreciate the amount of time and attention our technology has been given. But as we are introducing some fairly innovative approaches to encryption, compression, and authorization, we don't expect the industry to change overnight."

DECTEC's authorization and access control system was designed to provide programmers with independent control over a national subscriber base. S.U.N. descramblers can be cost effectively addressed by programmers or third party packagers without a centralized DBS authorization facility, thereby saving the industry million of dollars in DBS Center operation expenses. "Programmers can opt for independent control at anytime," explains Mr Grayson. "But in the interim, dish owners subscribing through the S.U.N. product will be authorized through third party distributors."

Distributor agreements are nonexclusive as are service and repair contracts which are available to companies who meet certain specified technical requirements. Because all of the parts within the S.U.N. decoder are off-the-shelf, the units can be repaired cost-effectively in the field by competent technicians. Distribution and Service information is available from Colin Ewart at 604-655-4463.

VCII and VCII Plus is a trade mark of the General Instrument division of Forstmann Little. Secure Universal Norm (S.U.N.) is a trade mark of DECTEC International Inc.

pr/clau.txt

THE SECURE UNIVERSAL NORM

Questions and Answers

The following are answers to some of the questions asked most about the SUN (Secure Universal Norm) scrambling system.

1. What distinguishes the SUN system from existing scrambling systems?

> *a. Open architecture*

The SUN system is software rather than hardware driven. The system's open architecture design is based on logic cell arrays (LCAs) to create an ever-changing adaptable platform through which SUN can be configured to emulate several encryption systems. The system can be reprogrammed while units are in-the-field, and users are able to customize networks to meet specific security and transmission requirements.

> *b. Enhanced security*

The SUN system can be programmed to utilize hard video encryption or sync inversion scrambling techniques. Where SUN differs from existing systems is that it protects encryption data codes with a super secure static RAM memory chip that is also used in the high level encryption process for German automatic banking systems. The SUN system offers more security than conventional scrambling techniques because it's constantly being upgraded by the manufacturer in order to maintain high level security in the face of improving technologies.

> *c. Flexibility*

The SUN system is flexible and customizable. While the system receives its operational instructions from the software loaded into six field programmable gate arrays (FPGAs), the software can be changed and re-configured to accommodate user preferences. Where hard scrambled video may be required by one operator, another may use the same SUN system to deliver daily newspapers to millions of subscribers.

2. What are some examples of SUN's flexibility?

> *a. Re-programmable System Interface*

SUN is equipped with the necessary logic to provide a customized video, audio and data scrambling system at a low cost and with little development time. In its basic form, SUN is equipped to emulate the conventional Videocipher scrambling scheme which presently serves most satellite programmers and over 2 million home satellite subscribers and cable

headends.

However, SUN can also be configured to emulate Oak Orion, BMAC, and Leitch scrambling designs, and the system can be programmed to work in several transmission environments including NTSC, PAL, SECAM, and some enhanced television formats, and digital compression schemes. Most interesting, however, is SUN's ability to store several scrambling designs and transmission formats within its configuration files and allow users to instantaneously switch between formats.

> *b. Unique Algorithm Schemes*

The SUN system offers the Data Encryption Standard as one of several algorithms available to users. Other than DES, operators may select any polynomial generator.

> *c. Re-programmable Audio Feature*

SUN can be configured to interface with Dolby digital as the entire audio processing section is re-programmable. However, compact disc (CD) quality audio is a standard feature in all units.

3. How does the SUN system function as a "Universal Norm"?

Fundamentally, the SUN system is a decryption interface designed to emulate most existing and future scrambling schemes as well as provide its own enhanced security protection. It allows consumers to switch between separately packaged and independently scrambled services without adding a second decoder. All system switching is transparent to the consumer.

Because SUN is not limited by firmware and is based on high-density re-programmable logic, it's design cannot be made obsolete. The SUN system is applicable world wide and can serve as a single system connecting countries served by different transmission formats and scrambling schemes.

4. How does SUN's reprogrammability function work and why haven't other vendors implemented the same technology?

SUN's patent pending design incorporates a small removeable snap in the circuit board which functions as a highly advanced "smart card". The "smart card" is a microprocessor recently developed by a States-based company which specializes in the design and manufacture of innovative security products for application throughout the world. When the "smart card" is reprogrammed, the data is automatically encrypted prohibiting everyone, including the operator, from reading the codes in the card.

We believe that no other vendor has developed a re-programmable encryption system for several reasons:

- The technology enabling reprogrammability in the encryption market has only been made available in the last two years. In fact, only this year has gate array technology achieved the speed and number of gates necessary to produce a mass marketable universal scrambling product. The conventional systems are based on decade-old technology which incurred heavy R&D costs. To scrap the old systems and begin development of a new technology from ground zero would require a substantial financial commitment from the product vendors.

- The development costs are very high. DECTEC spent four years designing the software for its SUN system.

- Conventional scrambling systems, which are monolithic by design, enable hierarchical marketing plans. Traditionally, when a scrambling system is sold to a user, only decoders manufactured by the encryption maker can be used in the user's network. Vendors close each other out of markets by selling firmware-based products.

5. What is unique about DECTEC's LCA approach?

DECTEC investigated state of the art mass production techniques using available LSI technology, but decided to invest in the more expensive, but much more flexible re-programmable gate array technique (LCAs). While the LCA approach proved immeasurably superior to an LSI design, developing SUN was not without its share of challenges:

As gate array technology is used in military, aerospace and radiology equipment applications, the approach is very new. Applying LCAs to a sophisticated consumer electronics product meant DECTEC required highly complex design programs which were not available. To further the development of a Secure Universal Norm, DECTEC's engineers created their own gate array design process to achieve the percentage gate use per array that allowed economic manufacture for a mass market.

6. What makes SUN's approach more secure than the conventional designs?

The answer concerns the weaknesses inherent in VLSI-based firmware in contrast to the benefits of logic-based software. On this level, the debate may seem somewhat esoteric, but it's one that has attracted much verbiage over the years.

> a. *VLSI Firmware vs. Logic-based Software*

In non-security based applications, VLSI designs are cheaper and provide a vendor greater control over his product in a particular market. But for products requiring the protection of extremely sensitive code, locking a product into firmware invites breaches in

the security. A product that can be reprogrammed in-the-field makes it virtually impossible for anyone to sustain access to the system. It's the difference between digging up treasure buried in one spot and finding a treasure chest that constantly moves.

> *b. Custom VLSI vs. Off-the-shelf Security Chip*

Where it may seem that custom designed integrated circuitry would be more secure than a product purchased from a catalog, we believe the reverse to be true.

Early on in the development of the Secure Universal Norm, DECTEC engineers found that the security field was not static. Developments in processors, algorithms, and interface architecture led us to Dallas Semiconductor which specializes in applying advances in security technology to products used in several different industries throughout the world. Dallas stays ahead of code breaking specialists by constantly improving the security of their products without affecting the general product specifications. It is in Dallas' best interest to maintain the highest integrity and most secure product line in order to serve its current and future customer base.

7. How is the SUN system scrambled?

> *a. Video*

The SUN video signal is inverted with sync pulses removed and replaced with data. The sync is restored by a timing generator driven by a crystal controlled phaselocked loop, with the fundamental initiation of this process triggered by a unique data pattern transmitted at field sync time. The encryption process is different from that employed by present systems because SUN's pattern detect circuit is in re-programmable LCAs rather than a custom IC. SUN's unique field sync pattern can be changed at will precluding unauthorized access by other systems.

Hard video encryption and digitized video can be programmed into existing SUN units, but the feature is not part of the system's basic field-programmable models.

> *b. Audio*

The stereo audio is pre-emphasized, digitized, then encrypted with a continuously changing keyword. The digitized information is then placed in bursts of data in the horizontal sync area. The entire audio processing section, from initial data recovery through descrambling, error correction and digital to analog conversion, is in re-programmable LCAs. This enables SUN's entire audio processing format to be changed while units are in-the-field. The complete format of the audio data, including method of re-creating keywords is flexible and reconfigurable.

8. How many channels can the SUN system handle and what is the speed of authorization?

The SUN System can hold 5,000 independent channels if configured as a "common" working key system. If, however, programmers look to independently controlled authorization centers, SUN's channel capacity would start at 256 channels. The number of channels available to the system is limited only by the on-board memory capacity of the removeable secure microprocessor in each consumer unit. The standard authorization rate is 1.2 million homes per minute.

9. How is authorization handled through SUN?

Authorization services available to users can be customized to match individual network requirements. For example, if a television programmer has a system in place and wishes to add authorization data in his own VBI and operate encryption and authorization from his own facility, then he may do so.

If, however, a programmer or business entity, would rather not take on the extra personnel and facilities required to run an authorization center, they may operate their network through a DECTEC Universal Teleport™. Also, several programmers may combine resources and operate a shared authorization center. DECTEC will also work with users who have an interest in setting up their own facility but require a transition and training period. Independent authorization centers can also elect to hook into a DECTEC Universal Teleport™ to insure cost-efficient redundancy.

10. What about special services like teletext and multiple audio channels for multi-lingual programming?

The SUN system can be configured as either a high speed data link with a corrected 4.8 Megabaud data capacity or 250 independent 19.2 Kilobaud channels.

The present SUN system delivers two independent channels of digital quality sound at 18 khz each. However, due to the reprogrammability of the system, users can configure the system to provide 4 channels at 9 khz each by adding time demultiplexers at minimal cost.

11. How does the SUN system handle Pay Per View?

The SUN system offers improved consumer specific data security and an on-chip credit balance system which is down loaded over the channel to the field units at a time not linked to the pay per view movie selected. SUN's thoughtful pay per view design removes the need for a massive fast response telephone network. SUN also offers an on-demand encryption feature which lets pay per view programmers air promos and movie trailers in the clear then select one of several scrambling schemes for any one movie. Through the SUN network, a programmer could relay a horse race to closed circuit sites via one scrambling mode and transmit a movie to cable homes or dish owners via a second or third scrambling method.

12. Can the SUN system help create a generation of field programmable IRDs (Integrated Receiver Decoders)?

Yes.

VOL. 8 ~ NO. 2 JUNE / JULY 1991

SIGNAL

THE VOICE OF CANADA'S SATELLITE INDUSTRY

EXCLUSIVE!

In-depth look at
S. U. N. Technology

CALGARY

SATELLITE SIGNS

WEST 91

SHOW GUIDE