

**NDS RADIOGUARD™ HD RADIO CONDITIONAL
ACCESS:**

**WHAT IT IS; HOW IT FITS IN THE BROADCAST
STATION; AND WHY IT WILL SUCCEED FOR
HD RADIO BROADCASTERS**

THOMAS RUCKTENWALD
NDS
Costa Mesa, California

NDS RADIOGUARD™ HD RADIO CONDITIONAL ACCESS: WHAT IT IS; HOW IT FITS IN THE BROADCAST STATION; AND WHY IT WILL SUCCEED FOR HD RADIO BROADCASTERS

THOMAS RUCKTENWALD

NDS

Costa Mesa, California

ABSTRACT

Conditional Access is the precise definition of the two words put together; access is based upon certain conditions. When applied to digital broadcasting, a consumer gets just what they want, no more and no less. This model works well for subscription pay services including pay TV.

So, how can this conditional access work for terrestrial HD Radio? How does such a system fit into a radio station environment and into radio station operations? Does terrestrial HD Radio have advantages over other transmission media? What programming works with conditional access?

This introductory paper examines, in understandable professional terms, the possible implementations of NDS RadioGuard™ Conditional Access for HD Digital Radio. NDS RadioGuard equipment fits into the station, mates to other equipment that may already be within the station, operates within the station's work flow, and creates new operations that the station must perform. This paper's explanations will allow all to comprehend the impact of this new and emerging radio broadcast capability. It suggests some business possibilities that may make conditional access implementation profitable.

WHAT IS CONDITIONAL ACCESS?

Under a conditional access system, reception of transmitted content only occurs when the receiver is authorized to receive the transmission and has the appropriate capability to decrypt the broadcast content. The receiver meets the broadcast conditions and provides access to the content.

Two main concepts embody the technology of conditional access: entitlement and scrambling. The entitlement is an authorization; the scrambling is an encryption of the content.

Entitlement is a right, privilege, or claim. In order to get an entitlement, the recipient must make a contract.

In a standard broadcast model, the consumer calls the provider or visits a website and supplies information.

They either already have or they arrange for receiver equipment and they order content, programming, or channels. The system handles everything automatically from this point forward, with entitlements based upon the arrangement transmitted from the provider to the correct and appropriate receiver only. The reception equipment knows what is supposed to receive and it provides the desired service.

Scrambling is mixing up or jumbling. For conditional access, such scrambling must be done so that the original content can be reconstructed without error or significant delay. The transmission side performs the scrambling, often using a known and standard type of methodology like 3DES or AES and a standard number of bits, like 128. Information about how to descramble the transmission is sent along with the content. The scrambling, while using a standard methodology, is an unknown due to frequent key changes and will not be decipherable unless the receiver is qualified by an entitlement. The scrambling key is dynamic and changes often over time. These keys, which are used to unlock the scrambling, are never sent directly, but are themselves disguised or encoded so that only a true and entitled receiver may enjoy the programming or content.

Both transmission and reception are a part of this ecosystem. The transmitter and the receiver have complimentary provisioning. The broadcaster transmits entitlements; the receiver recognizes only its own entitlements. The broadcaster transmits scrambled or encrypted programming; if entitled, the receiver can descramble or decrypt the programming.

HOW CONDITIONAL ACCESS WORKS FOR HD RADIO

In many conditional access implementations, the service is offered by one single platform supplier. That supplier provides all the services, the content or channels, and is the source for all the entitlements.

Examples include DirecTV for satellite TV, Cablevision for Cable TV, Qwest for IPTV, and Sirius for satellite radio. All content, all services, all entitlements, and all authorized equipment for that system originate from one source, the platform provider.

This is not and cannot be true for terrestrial digital radio. Content suppliers, radio stations, and station groups will continue to independently compete. A conditional access system for HD Radio must coordinate all of these entities, without business interference, so that any equipped receiver may possibly receive these broadcasts.

Every station or station group that deploys conditional access will have the same type of equipment and perform a similar scrambling process. At the same time, each station or station group must be uniquely distinct and recognizable by any equipped receiver. There can be no identity, channel identification, or programming ID duplication.

In order for the system to operate correctly, every radio must be uniquely identified so that its entitlements can be individually addressed to it. Consumers should receive only the programming that they desire and only the programming that is intended for them. Each radio or receiver must perform similarly with every broadcast source.

The best possible answer is to have something within the system that ties everything together. This portion of the system must provide unique station and conditional access service identification to each participating broadcaster. It must authenticate the broadcaster and then provide the information that differentiates the stations. This portion of the system also holds information about each unique equipped radio. It must be able to identify each unique radio and provide it information so that it will perform with the desired broadcast or content.

Such a system is shown in Figure 1. The system includes the existing HD Radio system Exciter,

Exporter, and Importer. Only channels created through the Importer may be encrypted as it is anticipated that the main program will remain free-to-air for station license purposes. The Importer will contain a new capability called the Scrambler. The Scrambler will be inert unless the conditional access equipment is in the system. The Scrambler can be used to encrypt multiple channels or programs simultaneously.

The conditional access system contains several operational components; the two main functions are the Entitlement Management Message Generator (EMMG) and the Entitlement Control Message Generator (ECMG). The EMMG generates Entitlement Management Messages (EMMs) which qualify individual radios. The EMMs are transmitted through the Importer on a low bit-rate data channel. The ECMG generates information about the scrambling keys. The Scrambler uses the keys to encrypt the content; the Entitlement Control Messages (ECMs) are transmitted through the Importer and to the receivers. The receivers use this information to recreate the control words that will descramble the content.

The ECMG, because of timing and associative reasons, must be co-located with the Importer at the station. The EMMG and the control over the system operation can be located anywhere, including a Network Operations Center (NOC) that would be built by a station group or service aggregator. A NOC can then control multiple stations and route entitlements to either a single or many definable stations. In this fashion, a station group or an aggregator can operate and control numerous stations in a cost efficient manner.

The portion of this system that ties competitive stations and all radio receivers into a cohesive unit is called the National Resource Manager (NRM). The NRM verifies station authenticity, provides unique conditional access service identification, verifies and signs radio entitlements, and holds the database of all radios.

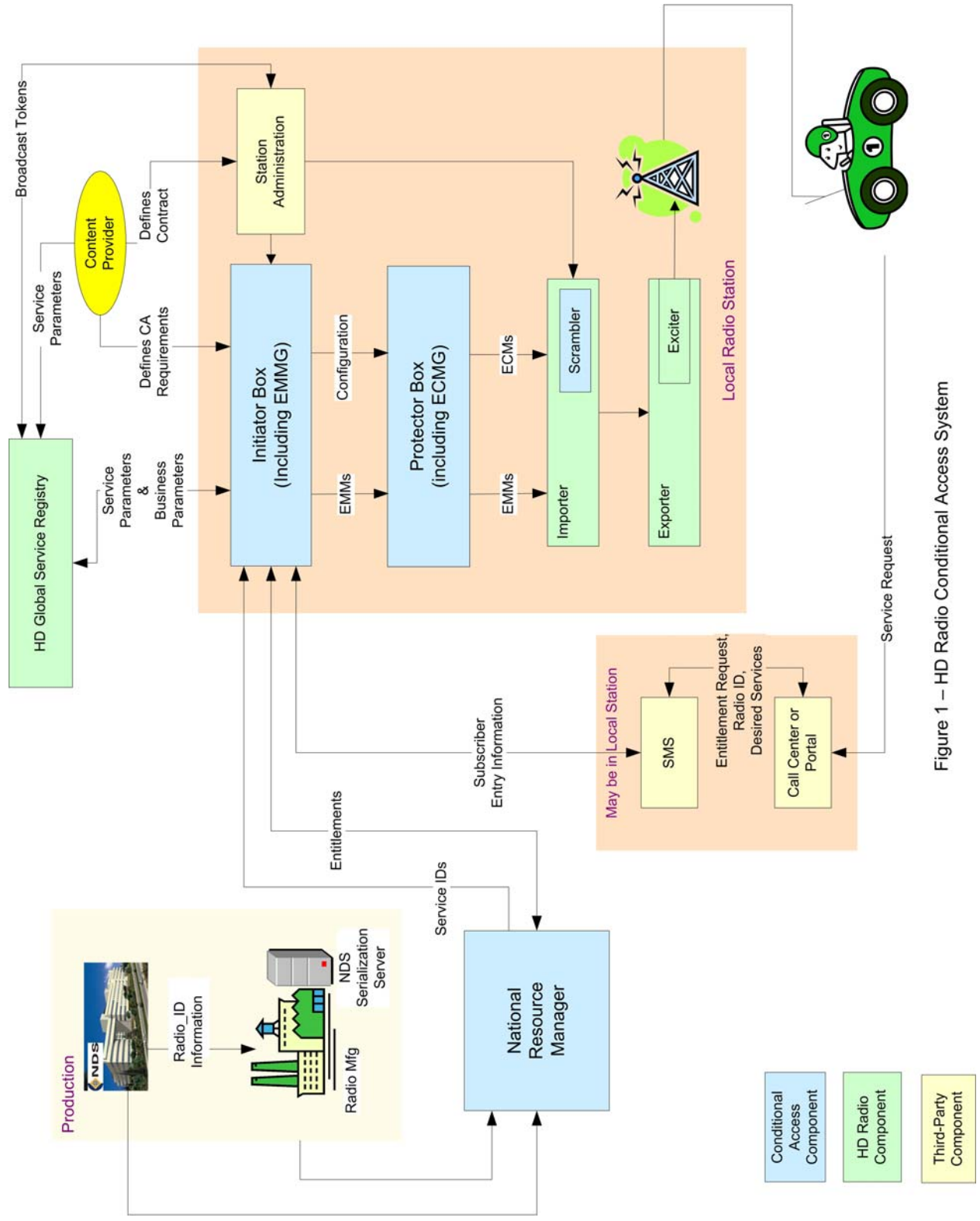


Figure 1 – HD Radio Conditional Access System

RADIOS AND RECEIVERS

This paper focuses on the broadcast implementation of conditional access. However, in order to understand the broadcast requirements, it is important to understand some basic radio requirements.

The radio must be able to decode or decrypt the scrambled content transmission in real time. In order to do that, the radio must know how the content was scrambled and it must already have the information it needs from the system to decrypt it. In a secure system, the information about descrambling and how the content was scrambled is only available to authorized receivers. The authorization comes from entitlements within the broadcast. Through an entitlement, the receiver knows that it is supposed to receive the scrambled signals and it knows how to obtain the descrambling information.

Addressing radios in a system that can receive from many broadcasting sources requires something special. Every radio must be unique to the system, even though the radios can come from many different manufacturers. The most efficient technology that makes every radio unique is serialization.

Each radio is uniquely serialized through the decoder chip. Each decoder chip contains some unique codes and with it, some embedded secrets. The chip/radio identification can be accessed through an activation sequence on the radio. When the consumer calls or registers via a website with the radio information, the system can identify the radio ID authenticity and individually address that radio.

The serialization information is provided to the decoder IC manufacturer by the conditional access manufacturer. The National Resource Manager also knows all the serialization information. Servers located at chip manufacturers and connected to the conditional access manufacturer will program the data that individualizes each HD Radio decoder chip. This process is done for other broadcast systems and is well known in integrated circuit manufacturing.

When the consumer wishes to register their radio and receive conditional access programming, they call the station or register with the online site. With the proper radio ID information, the receiver, within seconds, will obtain its entitlements and automatically turn on, as shown in Figure 2.

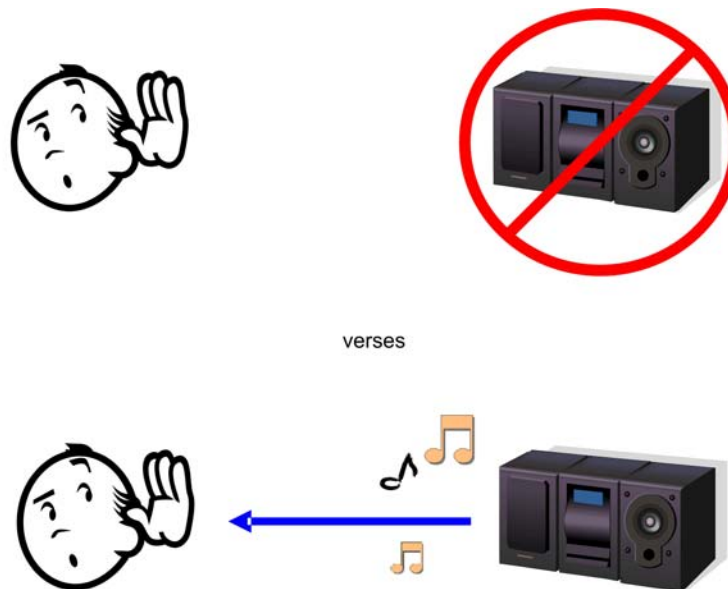


Figure 2 – Entitlements Allow the Encrypted Programming

A CONDITIONAL ACCESS SYSTEM WITHIN THE HD RADIO STATION ENVIRONMENT

The conditional access system created for HD Radio is called NDS RadioGuard™. It was created by NDS as a technological development in cooperation with iBiquity Digital Corporation, the licensors of HD Radio technology.

NDS RadioGuard equipment fits into the station, mates to other equipment that may already be within the station, operates within the station's work flow, and creates the new operations that the station requires.

This conditional access system will connect to the HD Radio Importer version 3.0 or higher. V3.0 contains the NDS RadioGuard scrambler module; previous versions do not have this capability and cannot be used for conditional access. The scrambler will be inert or inactive without a conditional access system. Once activated, the scrambler will continue to operate as last instructed, even if disconnected from the CA system.

For an individual station, the NDS RadioGuard Conditional Access System is embodied in two boxes.

The first box, called the NDS RadioGuard Protector, mates directly to and must be co-located with the HD Radio Importer. Within the Protector is the Entitlement Control Message Generator (ECMG), and the Entitlement Management Message Spooler, which is a

buffering and smart carousel transmission of radio entitlements.

The second box, termed the NDS RadioGuard Initiator, mates to the Protector and to the National Resource Manager. The Initiator can exist anywhere in the station environment. It contains the EMMG, a User Interface, setup and control over both its own operation and the Protector, the ability to enter information about radios that are authorized to receive from the station, and connectivity to and from the NRM for authorization, verification, and unique radio receiver communication.

The Initiator was first intended for single station operation. However, the unit can also control many stations and it can be placed in a central location, like a NOC. The Initiator may then set up and control the conditional access for many stations, through the Protector boxes, as shown in Figure 3. EMMs from the NOC-based Initiator EMMG are steered to the appropriate station or stations. This NOC-based Initiator connects to the NRM on behalf of all broadcast stations within its system.

If there is an Initiator at both a station and a NOC, the NOC makes submissions to the station. Content providers, such as Premier Radio or Westwood One, submit their content and conditional access parameters to the station group NOC-based Initiator or the station Initiator. This submission process provides control to the most local entity, preserving traditional US terrestrial broadcast radio localism.

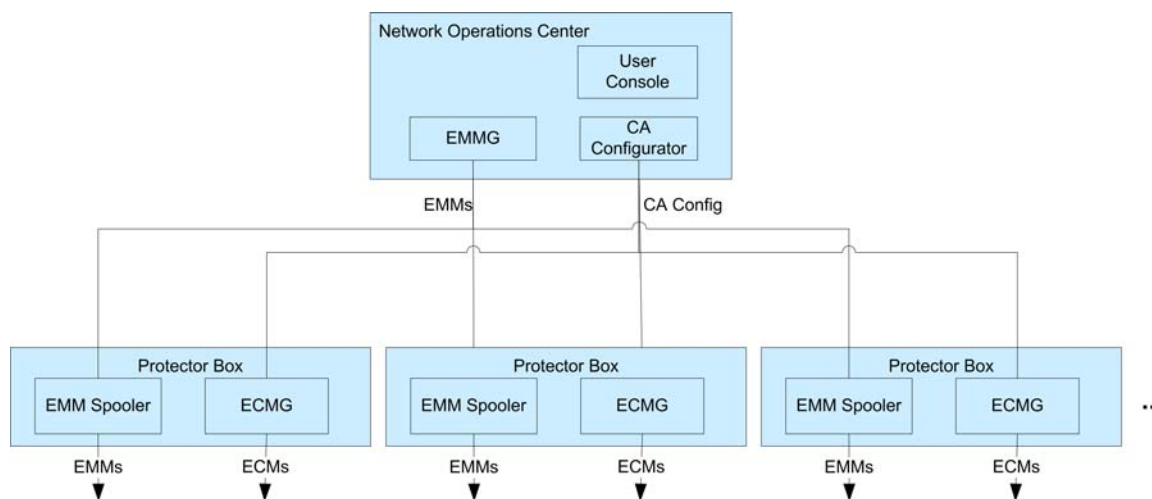


Figure 3 – A Network Operations Center Replaces the Initiator and Controls Multiple Station Protector Boxes

CONDITIONAL ACCESS OPERATIONS

Equipment setup for the NDS RadioGuard conditional access system will be straightforward. A structured entry of station information will activate the equipment.

Application of conditional access can be as simple as turning it on for specific multicast channels and leaving that to run until the station decides otherwise.

The system will also support constant change. Conditional access changes will require operational personnel to access the user interface. CA can be applied to specific programs or channels and changed at the discretion of the station operators. One program may be encrypted but the next program may be free-to-air.

Future automation systems will mate to NDS RadioGuard. Because of the new programming opportunities, automation systems will need to control multiple playlists and will also need to control additional station equipment. The automation system may provide one place to access and setup the entire station system.

Radio/receiver data entry is another operational requirement. When the consumer registers their radio, the radio ID information is the critical information for entitlement. However, this registration process is an important moment for the radio broadcaster. This is an opportunity to learn more about the consumer. That information will be extremely valuable for the station advertisers. Stations and station groups will have some free choice concerning what information is required for registration.

The standard NDS RadioGuard conditional access equipment will provide capability to entitle radios for the beginning of the station business or for the life of a small station. If the registered radios exceed several thousand, the station or station group should consider either a separate subscriber management system (SMS) or some subscriber or membership software that can be integrated with the conditional access system. Integration with most well-known SMS systems should be an easy process.

Radio registration information can be accepted as direct data entry from operations personnel or a contracted service, entries from an SMS system, or from a web portal that allows the user to self-register. Internet self-registration, once successfully integrated, may provide the lowest cost but may also prove frustrating when the Internet presents a potential barrier, or for those that do not understand the required radio equipment information.

THE NATIONAL RESOURCE MANAGER

The NRM is outside the station environment and is a facility supplied by NDS as the conditional access creator. It is not part of the radio station or station group. Every new station installation is verified by the NRM. Every request for radio entitlement is verified by the NRM. It is a very large database and is the source information for and about the system.

The National Resource Manager will be an equipment-redundant installation. As the conditional access system proliferates, there will be site redundancy.

Under most operations, the radio station or station group will never know that the NRM is in the system. The only time that the NRM is evident is when there is a problem. The primary problem will be that the radio receiver that is being registered does not have appropriate serialization. The consumer is trying to register a radio that is not part of the system.

DIGITAL TERRESTRIAL HD RADIO ADVANTAGES OVER OTHER TRANSMISSION MEDIA

It may be tempting to complain that each radio station allocation represents a narrow bandwidth and because there are already signals occupying that allocation, there is relatively little space for great accomplishments. However, the HD Radio system is proving such complaints unfounded.

HD Radio has shown how a digital overlay can perform tremendous service and that the digital signals can be grouped to provide multiple offerings even though there is an analog signal occupying the associated bandwidth. While there may be less transmission bit space per radio station than TV broadcasts, cable, or telephony, the over 13,000 active US terrestrial radio stations represent tremendous throughput. There is a roadmap to an all-digital station, which will provide even more bit space and greater opportunities.

Our population is already habitually involved in terrestrial radio. 233 million people listen to terrestrial radio an average of 19.5 hours per week. There are 230 million registered cars with radios; 17 million new cars are sold each year, virtually all with terrestrial radio. New models will include HD Radio. Approximately 70 million new radios were made last year and there are over 800 million radios in the US.

iBiquity, the creator of HD Radio, has had an opportunity to examine the successes and failures of other transmission media. It is easy to see that WebTV failed and that digital video recorders are a hit, although the penetration of such DVR devices is still statistically

low. The iPod is an audio experience; even Video iPod usage is 99% audio. An iPod device that can also receive content from a broadcast source may have significant value. The same companies that brought successful TV and Internet technology will bring successful HD Digital Radio technology.

Technology by itself does not guarantee success. Content is King. There will undoubtedly be some national offerings, particularly music from the larger organizations. Conditional access and digital rights management will be used for stored programming and will be particularly important for the music industry.

The biggest advantage for terrestrial broadcasting, particularly radio, is localism. Even with higher penetration of national offerings and increased speed in communication, people within a local area still value their hometown above all else. Morals and values in Peoria, Illinois are different than New York City. People in Texas like Friday night high school football and they want programming that speaks to their lives and to their neighborhood. While programming success might be spelled somewhat differently from one local community to the next, HD Radio is well positioned to accommodate this.

HD RADIO PROGRAMMING THAT WORKS WITH CONDITIONAL ACCESS

Satellite radio is primarily music programming with little to no commercials. Patrons pay for this jukebox-type service, with rates around \$13 per month. The success of satellite subscription radio is debatable.

Because terrestrial radio is traditionally a free service, one might expect that HD Radio subscription services would be the last thing to develop. While that may be true for music programming, one might expect data subscription services would be successful from inception. Traffic services are a good example of a data service. Radio signals are hearty and data transmitted to specific applications would require little bandwidth while providing maximum satisfaction. Conditional access is required to secure these subscription data services.

Public service may fuel early conditional access successes. Local Fire, Police, and Emergency Services may require a private emergency channel. The International Association of Audio Information Services (IAAIS) provides radio reading services for the blind. These readings include copyrighted books, newspapers, and magazines; under agreement, these must be offered only to those who have a sight impairment. Conditional access is required to maintain public service privacy.

Pay-per-listen events have high value. Concerts, in particular, seem to extract a strong positive consumer response. Special events of any kind, those that occur on a one-time basis, can provide a new source of revenue for terrestrial radio.

Membership has its privileges. For example, NPR stations can provide additional programming that is entitled only for its members. During pledge periods, where members receive pledge-free programming, the general public receives donation requests.

A most promising offering, however, seems to be “opt-in” services. Opt-in means that the consumer wishes to receive these program services and they make the appropriate arrangements to obtain them. The consumer pays no fees or subscriptions because the service or subscription is advertiser supported. Like cable TV or satellite subscription radio, such opt-in services may enjoy artistic freedom. Protected opt-in services, available only to those that subscribe through registration, could open up new avenues and programming opportunities. This may affect talk shows, comedy channels, and music that may not be available on a free-to-air station, as well as medical and religious programming.

While a decision specifically on this has not been obtained from the FCC prior to this paper’s publication, such a decision would be consistent with other rulings. This is a winning scenario for broadcasters, for the consuming public, and for the FCC. Terrestrial radio broadcasting will be able to offer programming that competes with its potential entertainment rivals; consumers that want this programming can obtain it while those that do not want it will never receive it or be bothered by the programming that they do not want to hear; the FCC, by allowing such broadcasts remains consistent with other rulings while at the same time reinforcing the intentions of free-to-air radio.

OUTSTANDING RETURN ON INVESTMENT

The radio station management might be tempted to ask “What is the Killer App?” and “What will be my return on investment in conditional access?”

The good news is that the conditional access system is flexible. It will support data transmission for applications as well as audio. It will support channels that are scrambled all the time as well as part-time and pay-per events.

The “killer app” is going to depend upon the offering, the local station, and the intended audience. For a blind person, the “killer app” is Radio Reading Services. For NPR, it may be membership benefits. For the hardcore commuter, it may be traffic information.

The offering that seems to extract the largest positive response from both broadcasting professionals and consumers involves opt-in. Opt-in continues the advertising-based model. Since the consumer is known, advertising is more valuable because it can be focused.

With opt-in, the radio station may have additional creative license and should be free to compete with and exceed satellite channels. For the consumer, receiving a free, fashionable service is extremely attractive.

While there are no predictive statistics for increased income or return on investment at this time, we believe that the broadcaster should, for a modest additional equipment investment in their present HD Radio installation, expect to double their present income with NDS RadioGuard HD Radio Conditional Access.

Pick an application or programming that you feel suits your station, community, and expected target audience.

CONCLUSIONS

NDS RadioGuard Conditional Access for HD Radio is a well-conceived offering that easily fits and integrates with compatible standard HD Radio equipment. One conditional access box provides the data for scrambling and data streams that will be used by the complimentary and entitled radio receiver. A second box registers users, enables entitlements, and provides setup and control over the conditional access system. NDS RadioGuard should be easy to install and set up. Operational requirements vary depending upon the desires of the station or station group, spanning from set up once to integrating with a subscriber management system or an automation system.

Conditional access also provides for new offerings and opportunities. This technology coupled with content or programming that may appeal to the local broadcast audience should deliver tremendous commercial success.

ACKNOWLEDGEMENTS

HD Radio is a registered trademark of iBiquity Digital Corporation

NDS RadioGuard is a trademark of NDS Ltd.

The Consumer Electronic Association for published radio statistics

Gershon Nachshon, Ron Katz, Katy Flores, and Patti Daino of NDS for their contributions to this paper