

# Pro:Idiom System Description

## Introduction and Summary

The Zenith Electronics copy protection system (Pro:Idiom) provides end-to-end cryptographic security for protecting digital HD and SD video (including movies) and music transmitted over existing private cable TV systems and private IP networks that are found in hotels, hospitals and other “hospitality” institutions. The operation of Pro:Idiom in these closed systems requires a license as does the manufacture of the in-room decryption devices. This licensing provides common industry restrictions both on the system operator as well as the manufacturer. These restrictions include compliance and robustness rules as well as encoding rules. During the development of the Pro:Idiom system a cryptology and digital cinema expert, Dr. Robert W. Baldwin was hired to help in the design and to ensure that sound design concepts were included in Pro:Idiom. An executive summary of Dr. Baldwin’s system review is included as Exhibit “C.” As outlined in Dr. Baldwin’s report there are a number of technical advantages to the Pro:Idiom system:

- “End to End” encryption – The content is protected at every step in the delivery chain
- All fixed keys are stored in hardware, unavailable to all levels of users
  - Guests
  - Hotel Operators
  - System providers
- Complete understanding of system, including trade secrets, is required to use “hacked”.

However, the biggest advantage in using the Pro:Idiom system is for the first time early release high definition content has been approved by studios for use in the hospitality industry.

Pro:Idiom requires equipment in guest rooms and an encryption server either within the facility or at the content provider’s Network Operations Center. A substantial benefit is that Pro:Idiom does not require any changes to the facility’s existing unidirectional TV cable or IP wiring and key management is handled in-band. 128 bit keys are passed in-band in AES encrypted form and fixed keys stored within the device are used to decrypt the bulk video keys which are in turn used to decrypt the video and audio stream.

A standard RF based Pay Per View (PPV) system is shown below in figure 1. In this example we have traditional over the air signals being received and re-transmitted on the hotel cable plant as depicted by the solid blue line. As this is publicly available content, no protection or restrictions are applied to the signal. Premium channels such as HBO-HD or ESPN-HD are received from a direct broadcast satellite or cable feed just as they would be in a consumer’s home, but Pro:Idiom encryption is applied prior to leaving the satellite receiver. The Pro:Idiom encrypted signal is then modulated and combined with the terrestrial signals and added to the hotel cable plant. This signal is represented

by the solid green line and the fact that it is Pro:Idiom encrypted is indicated by the dashed red line overlay. The final content source is video on demand, In this case Pro:Idiom encrypted movies are stored on a secure server and when a guest purchases content it, a physical television channel is assigned to transport the content to the room, the content is spooled out of the server on this channel and combined on the cable plant with the other forms of content. This is represented as the solid red line below with the Pro:Idiom encryption being represented by the dashed red line.

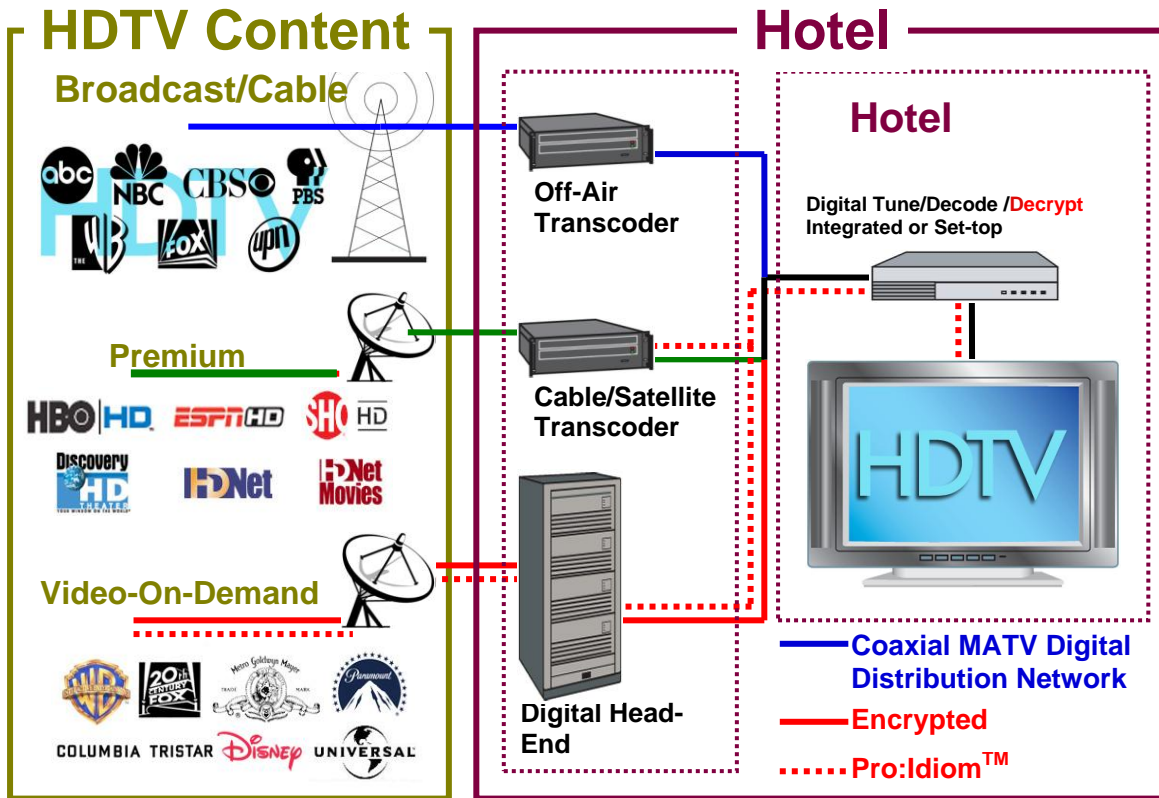


Figure 1

A closer look at these two Pro:Idiom content sources reveals the following. In the first case, satellite or cable fed premium content such as HBO-HD or ESPN-HD is real time encrypted in the Hotel Head-End Closet as shown in figure 2. In this example we receive the transport stream of the desired premium channel on a modified DirecTV or cable receiver, remove the conditional access, then re-format the stream into a standard ATSC compliant format and Pro:Idiom encryption is applied before it leaves the satellite receiver. The encrypted ATSC compliant stream is then modulated and sent to the television in the room. The in-room television receives the signal and decrypts the video prior to sending it to a standard MPEG decoder for video de-compression.

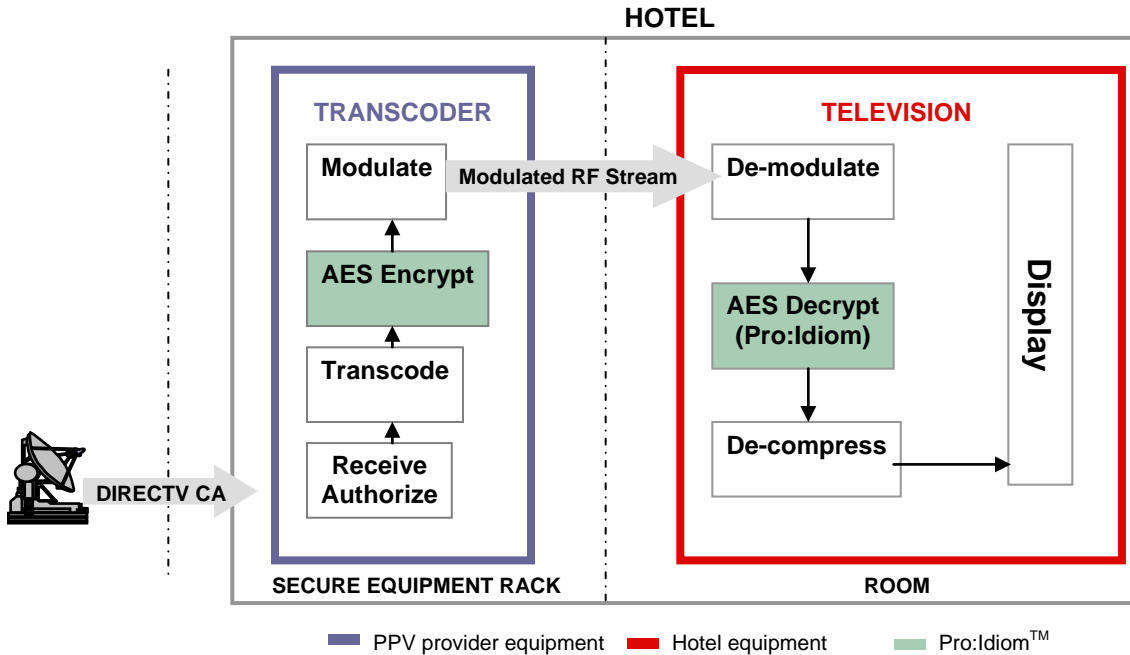


Figure 2

In the second mode, the content such as Pay-Per-View (PPV) movies are encrypted at the providers Network Operation Center (NOC) before being sent to the Hotel or Hospital, as shown in figure 3 below. In this case the encrypted content is sent by the PPV provider to a secure server at the hotel over a private satellite link and stored on a server in Pro:Idiom encrypted format. Movies when purchased are then sent to television in the room and decrypted by the television. One of the advantages is that separate key files are not stored on the server and no bandwidth is used in the encryption process.

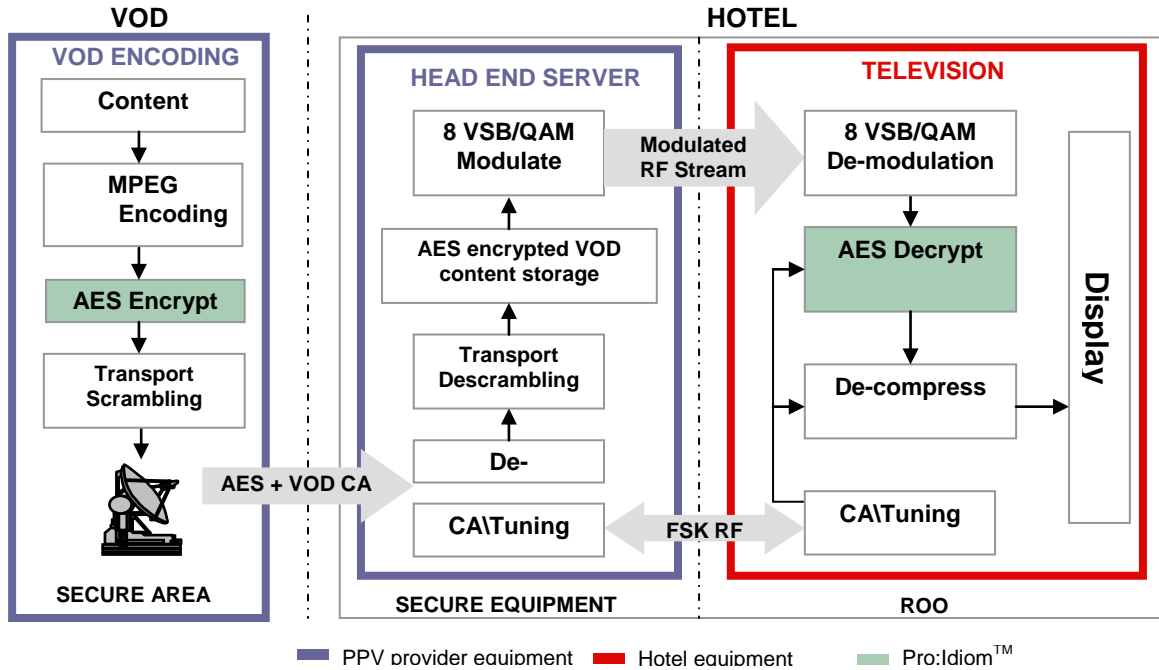


Figure 3

An example of a simplified architecture is outlined in figure 4 below. The STB would output MPEG transport stream from the 1394 connector using DTCP, the Pro:Idiom encryption module would receive this stream, update any relevant PSIP information and then re-encrypt with Pro:Idiom AES encryption. The encrypted signal would then be passed to a standard interface such as an ASI output or an RF modulator. An IP interface would be included to perform key renewal and other system maintenance activities. The whole system (STB, encryption module, etc) would be housed in the hotel's secure area to prevent unauthorized access to the equipment. This implementation is currently under development.

A cable head end based architecture is also currently available. In this version a real time encryptor with ASI in and ASI out is installed in the cable head end, and programs in the clear are routed through the Pro:Idiom encryption module prior to distribution on the cable plant typically on a fiber ring dedicated to "hospitality" locations.

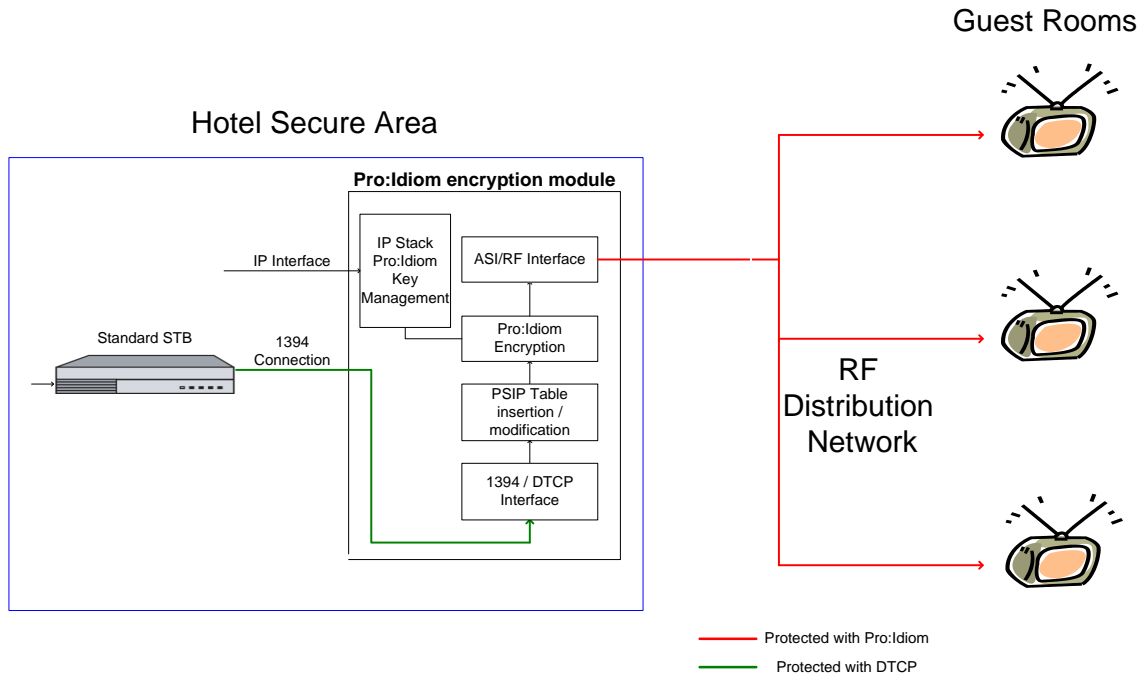


Figure 4

In the system outlined in figure 4 several system and licensing limitations have been imposed in order to prevent unauthorized access to the content. This implementation is currently under development.

A cable head end based architecture is also currently available. In this implementation a real time encryptor with ASI in and ASI out is installed in the cable head end, and programs in the clear are routed through the Pro:Idiom encryption module prior to distribution on the cable plant typically on a fiber ring dedicated to “hospitality” locations.

#### Authentication:

While Pro:Idiom does not include authentication, there are other key security aspects inherent in the use of Pro:Idiom which are not found in other consumer based systems like DTCP. Pro:Idiom system operation is only allowed under license on private networks within a limited field of use - “hospitality.” Thus, all devices on the network have been installed and authorized for use by the system operator and are under the control of the system operator. This is vastly different from a consumer network where unknown devices come and go on the network and devices remain in the possession of unknown consumers. While the network is “accessible” in the sense that a hacker may cut the wire and insert his device into the network, such efforts will fail for two reasons. First, the devices used on the network are specialized for the Hospitality industry by inclusion of a specific Pro:Idiom decryption Integrated Circuit (IC) that is not available to manufacturers except under a license which controls the sale, use and disposal of these decryption ICs. Secondly if the television or STB is somehow obtained it still requires authorization from the system provider for it to actually perform the decryption function.

Copy Control Information:

Copy control information is preserved and passed along unaltered to the television receiver. During the transmission it is encrypted like other elements of the system messages. To date no system provider or device manufacturer has plans for devices which would include storage capabilities. Pro:Idiom devices have traditionally been display only devices. Moreover, the Compliance Rules prohibit any copying on removable media. Any permitted copies are limited to particular devices.

Device Renewal

The Pro:Idiom system does include a renewal feature. The fixed keys within the device can be updated with a special "key renewal" command that is sent within the video stream. This feature not only allows for the keys to be changed if the system is compromised but also provides an option for different system operators to have different key sets in use, either at the system level or if need be on a hotel by hotel basis. The key renewal process is a contractual obligation for both manufacturer as well as system operator as part of the license agreement.

Licensing

Pro:Idiom is licensed to all qualified manufacturers, system operators and content providers on a royalty free, reasonable and non-discriminatory basis and the licenses are administered by Zenith Electronics Corporation. As indicated above the license includes compliance, robustness and encoding rules which can trigger liquidated damages if violated. To date there are well over 10 different licensees including the premiere hospitality vendors, Panasonic, Sharp, LGE, Philips and LodgeNet.

While Zenith does not purchase or license content, the following studios have granted Standard Definition and/or High Definition content distribution rights to LodgeNet, who use Pro:Idiom to protect this licensed content:

<b>Studio</b>
Columbia (Sony)
Disney
DreamWorks
Fox
Lion's Gate
Magnolia
MGM
New Line
Paramount
Universal
Warner

In addition the following premium satellite/cable content providers among others have granted high definition content distribution rights to LodgeNet using the Pro:Idiom system:

HBO  
ESPN  
Discovery Channel  
HD-Net

As an access control technology, circumvention of Pro:Idiom is fully subject to the remedies of the Digital Millennium Copyright Act (DMCA). Moreover, the system includes patent applications as well as trade secrets that provide added remedies against circumvention. Further in order to plug the “analog hole” no analog video outputs are allowed on devices, and only authorized digital outputs are allowed.

## **EXHIBIT “A”**

### **COMPLIANCE RULES**

#### **E.1 Generally**

**E.1.1 Definitions.** Capitalized terms in this Exhibit have the meaning set forth in the applicable Pro:Idiom Agreement.

**E.1.2 Use of Pro:Idiom.** Pro:Idiom is an encryption technology for encryption of MPEG compliant stream to protect premium audiovisual content. Pro:Idiom Agreements do not define when Pro:Idiom must be applied to content to be transmitted in the Hospitality Environment. The obligation to use Pro:Idiom may be imposed by (i) provider of particular content; (ii) law or regulation; (iii) other sources of the content (e.g., a prior content protection technology or conditional access system).

**E.1.3 Limitation on Use of Pro:Idiom.** Pro:Idiom may only be used to encrypt Commercial Audiovisual Content with the CCI state of (i) Copy Never, Copy One Generation, or Copy No More.

**E.2 Rules Governing Licensed Products Containing Pro:Idiom Sink Functions.** The rules in this Section E.2 apply to Pro:Idiom Licensed Product containing a Pro:Idiom Sink Function with respect to Pro:Idiom Protected Content received by that Pro:Idiom Sink Function.

**E.2.1 Inspection of CCI.** Upon receiving Commercial Audiovisual Content, a Pro:Idiom Licensed Product must inspect the system header message, as defined in the Specification, and transmit the CCI such that the CCI instructions may be implemented accordingly.

#### **E.2.2 Output Control Rules**

**E.2.2.1 Analog Outputs.** A Pro:Idiom Licensed Product may not transmit Decrypted Pro:Idiom Content through an analog output.

**E.2.2.2 Digital Outputs.** In the territory of the United States and all territories other than those governed by Section E.2.2.3:

(a) Decrypted Pro:Idiom Content with the state Copy Never shall not be transmitted out of a Pro:Idiom Licensed Product using any digital output technology except for uncompressed digital output technologies that are approved, at the time of manufacturing of the Pro:Idiom Licensed Product, for use in “Unidirectional Cable Products” for the output of “Controlled Content” (as those terms are defined in the DFAST License).

(b) Decrypted Pro:Idiom Content with the state Copy One Generation or Copy No More shall not be transmitted out of a Pro:Idiom Licensed Product using any digital output technology except for digital output technologies that are approved, at the time of manufacturing of the Pro:Idiom Licensed Product, for use in “Unidirectional Cable Products” for the output of “Controlled Content” (as those terms are defined in the DFAST License).

(c) When transmitting Decrypted Pro:Idiom Content using an approved digital output technology, a Pro:Idiom Licensed Product shall cause the digital output technology to encode the data with the appropriate encoding for content marked with the applicable state and shall comply with any associated obligations imposed under the DFAST License to the same extent as a Unidirectional Cable Product passing Controlled Content to such an output.

**E.2.2.3 Digital Outputs in Certain Territories.** In territories other than the United States, where the government has regulated digital output technologies for use with cable or satellite broadcast of television signals, Decrypted Pro:Idiom Content with the states Copy Never, Copy No More or Copy One Generation shall not be transmitted out of a Pro:Idiom Licensed Product using any digital output protection technology except for digital output technologies that are approved by such government for use with content marked with such states in compliance with any associated obligations that are imposed by such government.

### **E.2.3 Record Control Rules**

**E.2.3.1 Copy Never Content.** A Pro:Idiom Licensed Product shall not permit the recording of Pro:Idiom Protected Content or Decrypted Pro:Idiom Content with the state Copy Never or Copy No More except (i) for Transitory Storage, or (ii) a period of up to 90 minutes in order to enable the delayed display of the content using a method permitted in Section E.2.3.3, with the applicable period determined on the basis of a unit of content data not exceeding one minute.

**E.2.3.2 Copy One Generation Content.** A Pro:Idiom Licensed Product shall not permit the recording of Pro:Idiom Protected Content or Decrypted Pro:Idiom Content with the state Copy One Generation except (i) for Transitory Storage, or (ii) using a method permitted in Section E.2.3.3.

### **E.2.3.3 Permitted Copying Methods.**

**E.2.3.3.1 Generally.** Any copy permitted by Sections E.2.3.1 and E.2.3.2 must be made using a method that uniquely associates the copy with the Pro:Idiom Licensed Product making the copy, so that it cannot be played on any other device and so that no further usable copies may be made of it (other than copies made from an output permitted by this Agreement), and on a medium that cannot be removed from the Pro:Idiom Licensed Product without damaging the Pro:Idiom Licensed Product by an ordinary consumer using general purpose tools or equipment that are widely available.

**E.2.3.3.2 Incrementing CCI for Copy One Generation.** A copy permitted by Section E.2.3.2 may continue to carry the CCI state of Copy One Generation for a period of up to 90 minutes from the initial making of that copy, with the applicable period determined on the basis of a unit of content data not exceeding one minute. Thereafter, the CCI associated with the content shall be modified so that it carries the state Copy No More.

## **EXHIBIT "B"**

### **ROBUSTNESS RULES**

#### **G.1. Construction.**

**G.1.1 Generally.** Pro:Idiom Licensed Products as shipped shall be designed and manufactured in a manner to effectively frustrate attempts to modify such Pro:Idiom Licensed Products to defeat the Compliance Rules or functions of Pro:Idiom.

**G.1.2 Defeating Functions.** Pro:Idiom Licensed Products shall not include (i) switches, buttons, jumpers or software equivalents of any of the foregoing, (ii) specific traces that can be cut, or (iii) service menus or functions (including remote-control functions), in each case by which Pro:Idiom or the Compliance Rules can be defeated or by which Pro:Idiom Protected Content can be exposed to unauthorized copying.

**G.1.3 Keep Secrets.** Pro:Idiom Licensed products shall be designed and manufactured in a manner to effectively frustrate attempts to discovery or reveal (i) the fixed keys, (ii) intermediate cryptographic values; or (iii) the methods and cryptographic algorithms used to generate or modify the fixed keys or bulk keys.

**G.1.4 Evaluation.** Before releasing any Pro:Idiom Licensed Products, Licensee must comply with Section 3.3 of the Agreement by performing or having performed, tests and analyses to assure compliance with this Exhibit G. Licensee is strongly advised to review carefully the Specification, the Compliance Rules and this Exhibit G so as to evaluate thoroughly both its testing procedures and the compliance of its Pro:Idiom Licensed Products. In addition to the foregoing, a self-certifying Licensee must complete the

Implementation Questions listed in G.4, submit that document to Zenith upon request, and preserve a copy of that document for its records.

**G.2 Protected Content Paths.** Pro:Idiom Protected Content shall not be available on outputs other than those specified in the Compliance Rules, and, within such Pro:Idiom Licensed Products, Pro:Idiom Protected Content shall not be present on any User Accessible Buses (as defined below) in non-encrypted, compressed form. Similarly unencrypted keys used to support any content encryption and/or decryption in the Licensed Protects' data shall not be present on any user accessible buses.

Notwithstanding the foregoing, compressed audio data may be output to an external Dolby Digital decoder in the clear via the S/PDIF connector. This section shall not apply to navigation data contained in the Program Association Tables (PAT) or the Program Map Tables (PMT). A "User Accessible Bus" means a data bus that is designed for SmartCard, PCMCIA, or Cardbus, but not memory buses, CPU buses and similar portions of a device's internal architecture.

**G.3 Methods of Making Functions Robust.** Pro:Idiom Licensed Products shall use at least the following techniques to make robust the functions and protections specified in this Agreement:

**G.3.1 Distributed Functions.** The portions of the Pro:Idiom Licensed Products that perform authentication decryption and MPEG (or similar) decoding shall be designed and manufactured in a manner associated and otherwise integrated with each other such that Pro:Idiom Protected Content in any usable form flowing between these portions of the Pro:Idiom Licensed Products shall be secure to the level of protection described in Section 3(e) below from being intercepted or copied.

**G.3.2 Software.** This subsection shall apply if these rules are amended to permit software implementation. Any portion of the Pro:Idiom Licensed Products that implements a part of Pro:Idiom in software shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. For the purposes of this Exhibit C, "Software" shall mean the implementation of the functions as to which this Agreement requires a Pro:Idiom Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in hardware. Such implementations shall:

(i) Comply with Section 1.3 by any reasonable method including but not limited to encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and in every case of implementation in software, using effective techniques of obfuscation to disguise and hamper attempts to discover the approaches used;

(ii) Be designed to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of features or characteristics, or

interruption of processing, relevant to Sections 1 and 2 of this Exhibit G. This provision requires at a minimum the use of code with a cyclic redundancy check that is further encrypted with a private key or a secure hashing algorithm or an equivalent level of protection such as encryption with a private key or a secure hashing algorithm; and

- (iii) Meet the level of protection outlined in Section 3.3 below.

**G.3.3 Hardware.** Unless and until this Agreement is amended, Pro:Idiom shall be implemented in hardware. Any portion of the Pro:Idiom Licensed Products that implements a part of Pro:Idiom in hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit G. Such implementations shall:

- (i) Comply with Section 1.2 by any reasonable method including but not limited to: embedding keys, key generation methods, key modification methods and the cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or the techniques described above for software;

- (ii) Be designed such that attempts to reprogram, remove or replace hardware elements in a way that would compromise the security or content protection features of Pro:Idiom or in Pro:Idiom Licensed Products would pose a serious risk of damaging the Pro:Idiom Licensed Product so that it would no longer be able to receive, decrypt or decode Protected Content. By way of example, a component that is soldered rather than socketed may be appropriate for this means; and

- (iii) Meet the level of protection outlined in Section 3.5 below.

For purposes of these Robustness Rules, “hardware” shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Pro:Idiom Licensed Product be compliant and that (x) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (y) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Pro:Idiom Licensed product or Pro:Idiom Component and such instructions or data are not accessible to the end user through the Pro:Idiom Licensed Product or Pro:Idiom Component.

**G.3.4 Hybrid.** This subsection shall apply if these rules are amended to permit software implementation. The interfaces between hardware and software portions of a Pro:Idiom Licensed Product shall be designed so that they provide a similar level of protection which would be provided by a purely hardware or purely software implementation as described above.

**G.3.5 Level of Protection.** Encryption functions of Pro:Idiom (including maintaining the confidentiality of keys, key generation methods, key modification methods and the cryptographic algorithms, conformance to the Compliance Rules and preventing

compressed Pro:Idiom Protected Content that has been unencrypted from copying or unauthorized viewing) shall be implemented in a way that they:

(i) Cannot be reasonably foreseen to be defeated or circumvented merely by using general purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons (“Widely Available Tools”), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or de-compilers or similar software development tools (“Specialized Tools”), other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required (“Circumvention Devices”); and

(ii) Can only with difficulty be defeated or circumvented using professional tools or equipment (excluding Circumvention Devices and professional tools or equipment that are made available only on the basis of a non-disclosure agreement), such as logic analyzers, chip disassembly systems, or in-circuit emulators or other tools, equipment, methods or techniques not included in the definition of Widely Available Tools and Specialized Tools in subsection (i) above.

**G.3.6 Advance of Technology.** Although an implementation of a Pro:Idiom Licensed Product when designed and shipped may meet the above standards, subsequent circumstances may arise which had they existed at the time of design of a particular Pro:Idiom Licensed Product would have caused such products to fail to comply with this Exhibit G and to pose a risk of substantial and imminent harm to the protection afforded by Pro:Idiom or Pro:Idiom Licensed Products (“New Circumstances”). If Licensee has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (occurrence of (a) or (b) hereinafter referred to as “Notice”), then within eighteen (18) months after Notice Licensee shall cease distribution of such Pro:Idiom Licensed Product and shall only distribute Pro:Idiom Licensed Products that are compliant with this Exhibit G in view of the then-current circumstances.

## **Exhibit “C”**

# **Security Assessment of LG Electronics Pro:Idiom™ copy protection system**

Dr. Robert W. Baldwin  
Plus Five Consulting, Inc.

## **Executive Summary**

The Zenith Electronics copy protection system (Pro:Idiom) provides end-to-end cryptographic security for protecting digital movies and music transmitted over existing cable TV systems that are found in hotels, hospitals and other institutions. Pro:Idiom requires equipment in guest rooms and an encryption server either within the facility or at the content provider’s Network Operations Center. A substantial benefit is that Pro:Idiom does not require any changes to the facility’s existing unidirectional TV cable wiring. This report presents a security assessment of the LG Pro:Idiom system performed by an independent security consulting firm, Plus Five Consulting. It provides sufficient technical detail to enable other security experts to understand the LG Pro:Idiom system and confirm our conclusions.

## **Primary Conclusions**

- The system prevents the theft of content by all attackers who only have access to household tools even if they have instructions written by experts.
- The system makes theft of content very difficult for experienced attackers, such as a graduate student in electrical engineering with access to all the equipment found in a university laboratory.
- The security of the system does not rely on the trustworthy behavior of hotel operators, room equipment installers, or hotel guests.

## **Technical Conclusions**

- Video output recording thwarted by compliance rules and HDCP encryption.
- The system thwarts tampering with Copy Protection control bits.
- The system only uses standard, well respect, cryptographic algorithms and its uses those algorithms in appropriate ways, and the system implements good management techniques for cryptographic keys.

- The system includes a small number of security mechanisms that can be protected by trade secrets and patents to ensure that only licensees can create interoperable systems. These proprietary mechanisms do not weaken the security of the standard cryptography and present a reverse-engineering barrier to attackers.
- The system can be renewed to respond to a major compromise.

In summary, Zenith's Pro:Idiom system provides high quality security that is appropriate for protecting premium content.

*Robert W. Baldwin* received a Ph.D. in computer security from MIT in 1987. He designed and built security products for Oracle, Tandem, LAT, and RSA Security. After four years as a Technical Director at RSA, he co-founded Plus Five Consulting in 1999 to provide design and review services that help companies quickly add effective security features to their products. His clients include governments, multi-national companies, network infrastructure providers, media providers, makers of handheld computers and small start-up companies.