ENCRYPTING SPI INTELLIHEAD
TECHNICAL REFERENCE MANUAL

PART NUMBER 99875352-2

OCTOBER 2007

MAGTEK®

REGISTERED TO ISO 9001:2000

20725 South Annalee Avenue
Carson, CA 90746
Phone: (310) 631-8602
FAX: (310) 631-3956
Technical Support: (651) 415-6800
www.magtek.com

REVISIONS

Rev Number	Date	Notes
1.05	8 Mar 07	Preliminary Release
1.06	27 July 07	Initial Release
2.01	10 Oct 07	Added specifications for SPI interface; clarified CS operation

LIMITED WARRANTY

MagTek warrants that the products sold to Reseller pursuant to this Agreement will perform in accordance with MagTek's published specifications. This warranty shall be provided only for a period of one year from the date of the shipment of the product from MagTek (the "Warranty Period"). This warranty shall apply only to the original purchaser unless the buyer is authorized by MagTek to resell the products, in which event, this warranty shall apply only to the first repurchase.

During the Warranty Period, should this product fail to conform to MagTek's specifications, MagTek will, at its option, repair or replace this product at no additional charge except as set forth below. Repair parts and replacement products will be furnished on an exchange basis and will be either reconditioned or new. All replaced parts and products become the property of MagTek. This limited warranty does not include service to repair damage to the product resulting from accident, disaster, unreasonable use, misuse, abuse, customer's negligence, Reseller's negligence, or non-MagTek modification of the product. MagTek reserves the right to examine the alleged defective goods to determine whether the warranty is applicable.

Without limiting the generality of the foregoing, MagTek specifically disclaims any liability or warranty for goods resold in other than MagTek's original packages, and for goods modified, altered, or treated by customers.

Service may be obtained by delivering the product during the warranty period to MagTek (20801 S. Annalee Ave., Carson, CA 90746). If this product is delivered by mail or by an equivalent shipping carrier, the customer agrees to insure the product or assume the risk of loss or damage in transit, to prepay shipping charges to the warranty service location and to use the original shipping container or equivalent. MagTek will return the product, prepaid, via a three (3) day shipping service. A Return Material Authorization (RMA) number must accompany all returns.

MAGTEK MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND MAGTEK DISCLAIMS ANY WARRANTY OF ANY OTHER KIND, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

EACH PURCHASER UNDERSTANDS THAT THE MAGTEK PRODUCT IS OFFERED AS IS. IF THIS PRODUCT DOES NOT CONFORM TO MAGTEK'S SPECIFICATIONS, THE SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT AS PROVIDED ABOVE. MAGTEK'S LIABILITY, IF ANY, TO RESELLER OR TO RESELLER'S CUSTOMERS, SHALL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID TO MAGTEK BY RESELLER UNDER THIS AGREEMENT. IN NO EVENT WILL MAGTEK BE LIABLE TO THE RESELLER OR THE RESELLER'S CUSTOMER FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE SUCH PRODUCT, EVEN IF MAGTEK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

LIMITATION ON LIABILITY

EXCEPT AS PROVIDED IN THE SECTIONS RELATING TO MAGTEK'S LIMITED WARRANTY, MAGTEK'S LIABILITY UNDER THIS AGREEMENT IS LIMITED TO THE CONTRACT PRICE OF THE PRODUCTS.

MAGTEK MAKES NO OTHER WARRANTIES WITH RESPECT TO THE PRODUCTS, EXPRESSED OR IMPLIED, EXCEPT AS MAY BE STATED IN THIS AGREEMENT, AND MAGTEK DISCLAIMS ANY IMPLIED WARRANTY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

MAGTEK SHALL NOT BE LIABLE FOR CONTINGENT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES TO PERSONS OR PROPERTY. MAGTEK FURTHER LIMITS ITS LIABILITY OF ANY KIND WITH RESPECT TO THE PRODUCTS, INCLUDING ANY NEGLIGENCE ON ITS PART, TO THE CONTRACT PRICE FOR THE GOODS.

MAGTEK'S SOLE LIABILITY AND BUYER'S EXCLUSIVE REMEDIES ARE STATED IN THIS SECTION AND IN THE SECTION RELATING TO MAGTEK'S LIMITED WARRANTY.

FCC WARNING STATEMENT

This equipment has been tested and found to comply with the limits for Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. Changes or modifications not expressly approved by MagTek could void the user's authority to operate the equipment.

FCC COMPLIANCE STATEMENT

This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference; and (2) this device must accept any interference received, including interference that may cause undesired operation.

CANADIAN DOC STATEMENT

This digital apparatus does not exceed the Class B limits for radio noise for digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de las classe B prescrites dans le Réglement sur le brouillage radioélectrique édicté par les ministère des Communications du Canada.

CE STANDARDS

Testing for compliance to CE requirements was performed by an independent laboratory. The unit under test was found compliant to Class B.

UL/CSA

This product is recognized per Underwriter Laboratories and Canadian Underwriter Laboratories 1950.

RoHS STATEMENT

When ordered as RoHS compliant, this product meets the Electrical and Electronic Equipment (EEE) Reduction of Hazardous Substances (RoHS) European Directive 2002/95/EC. The marking is clearly recognizable, either as written words like "Pb-free" or "lead-free", or as another clear symbol ( ).

TABLE OF CONTENTS

TABLES AND FIGURES

SECTION 1. FEATURES AND SPECIFICATIONS

The Encrypting SPI IntelliHead™ provides secure three-track magstripe reading capabilities for use in POS terminals and other applications where system requirements dictate the need for improved security to meet PCI (Payment Card Industry) requirements. The readers incorporate the MagTek Triple-track ***Delta ASIC***. The serial output from the Delta ASIC is encrypted before it leaves the encapsulated head to ensure the same level of security applied to other types of financial transactions.

This family of Encrypting IntelliHead Readers utilizes TDEA (a.k.a. Triple-DES) encryption with a unique key per device to encrypt the magnetic track information. The Encrypting IntelliHeads are available in a variety of spring and beam arrangements for both swipe and insert reader configurations. The three-track heads conform to ISO and AAMVA standards.

The SPI (Serial Peripheral Interface) is a synchronous full-duplex serial bus used for communication between the Reader and the target system.

FEATURES

Major features of the Encrypting IntelliHead include:

- Bi-directional card reading
- Reads up to three tracks of card data that meets ANSI/ISO/AAMVA/JIS standards
- All electronics are potted inside the head to prevent tampering
- Includes Device Serial Number
- All card data from the triple-track Delta ASIC is encrypted using TDEA prior to transmission (the data is not decoded or formatted prior to encryption)
- Uses a unique double-length DES key per device
- SPI bus compatible 2 to 5 wire serial interface
- Maximum SPI bus transfer rate of 100 Kbits/Second

CONFIGURATIONS

The reader configurations are as follows:

Part Number	Description	Cable Length and Connector Type	For use with
21030033	Butterfly spring	125mm, 8-pin Molex 51021	90mm & 100mm Swipe Readers
21030034	Beam arm 5.08mm	125mm, 8-pin Molex 51021	IntelliStripe 60 models
21030035	Beam arm 4.05mm	125mm, 8-pin Molex 51021	IntelliStripe 70 models
21030038	Accordion spring	125mm, 8-pin Molex 51021	60mm Slim Profile Readers
21030039	43mm spring	125mm, 8-pin Molex 51021	43mm Readers
21044012	43mm Rail	125mm, 8-pin Molex 51021	N/A
21045093	90mm Standard Rail	125mm, 8-pin Molex 51021	N/A
21046008	60mm Slim Profile Rail	125mm, 8-pin Molex 51021	N/A
21047023	90mm Slim Profile Rail	125mm, 8-pin Molex 51021	N/A
21160128	IntelliStripe 60 Front & Side Bezel	125mm, 8-pin Molex 51021	N/A
21160129	IntelliStripe 60 Front Bezel	125mm, 8-pin Molex 51021	N/A
21160133	IntelliStripe 60 Side Bezel w/ Latch	125mm, 8-pin Molex 51021	N/A
21170011	IntelliStripe 70 Side Bezel	125mm, 8-pin Molex 51021	N/A

REFERENCE DOCUMENTS

Triple Track ASIC With Shift-Out, 3V, Specifications, P/N 99875337
Magnetic Card Reader Design Kit Technical Specification, P/N 99821002
ANS X9.24-2004 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

SPECIFICATIONS

Table 1-2 lists the specifications for the Encrypting SPI IntelliHead.

Table 1-2. Specifications

Reference Standards	ISO 7810 and ISO 7811; AAMVA*
Recording Method	Two-frequency coherent phase (F2F)
Message Format	Bit serial
Card Speed	4 to 60 ips (10.1 to 152.4 cm/s)
Flammability	Meets UL94V-0
ELECTRICAL	
Voltage	2.7-3.6 VDC
Current	4.5mA nominal when idle, 12mA maximum when active. The device is idle when no card is being swiped and no SPI commands are being processed, otherwise it is active. The device is typically idle most of the time.
ENVIRONMENTAL	
Temperature	
Operating	-40 °C to 70 °C (-40 ^{o}F to 158 ^{o}F)
Storage	-40 ^{o}C to 70 ^{o}C (-40 ^{o}F to 158 ^{o}F)
Humidity	
Operating	10% to 90% noncondensing
Storage	10% to 90% noncondensing
Altitude	
Operating	0-10,000 ft. (0-3048 m.)
Storage	0-50,000 ft. (0-15240 m.)

* ISO (International Standards Organization) and AAMVA (American Association of Motor Vehicle Administrators).

SECTION 2. SPI OPERATION

This section describes the SPI (Serial Peripheral Interface), the SPI bus interface timing, communication protocol, timeouts, and data output format. For a description of abbreviations see Appendix A. *Glossary Of Terms*.

SPI INTERFACE

The interface supports a bidirectional communication scheme and provides a means of selecting the reader—for applications that incorporate multiple SPI devices—by using the Chip Select line.

The signals used on the interface are shown in Table 2-1.

Table 2-1 Interface Connector

Pin Number	Signal Name	Description
1	SCL	Serial Clock Input
2	SDO	Serial Data Output
3	SDI	Serial Data Input
4	DAV	Data Available (output)
5	CS/	Chip Select (negative true)
6	VIN	Voltage input
7	GND	Logic Ground
8	Head Case GND	Frame Ground

The connector is a Molex 51021-8000 which mates with a number of housings in the Molex product line (e.g., 51047, 53047, 53048, 53261, and 53398).

The SPI interface can be thought of as a variable-byte parallel to serial shift register. A variable number of data bytes are transmitted serially in 8-bit groups in the order of MSB to LSB.

For example, the bit transmission order for consecutive bytes A and B would be:

A(bit 7) A(bit 6) … A(bit 0) B(bit 7) B(bit 6) … B(bit 0)

The host is the master of the SPI bus and this device is the slave. The master controls the clock and decides when data will be exchanged on the SPI bus. Data is always sent in both directions, from the master to the slave and from the slave to the master at the same time.

The SCL signal is the serial clock input for the device. This signal is sent from the host (master) to the device (slave). A bit of data is exchanged between the host and the device, in both directions, each clock period. When the host does not want to exchange data it keeps the clock idle.

The SPI interface can be configured to use any of the four combinations of clock phase and clock polarity. The device defaults to clock phase = 0 and clock polarity = 0 which means that the data is centered on the first edge of the clock period and that the clock line is low when idle. In this configuration, the data is clocked on the rising edge of the clock. When the clock polarity is set to 1, the data is centered on the second edge of the clock period. When the clock polarity is set to 1, the clock line is high when idle. See the SPI clock phase and polarity property for details on how to adjust the clock phase and polarity. This signal is required to read card data from the device.

The SDO signal is the serial data output for the device. This signal is sent from the device (slave) to the host (master). This signal is required to read card data from the device. When the CS/ (chip select) signal is not asserted (high) the SDO signal is put in a high-impedance state. Immediately after the device is power cycled or reset this signal is in an indeterminate state for a maximum of 1 second. This signal should be ignored during this time.

The SDI signal is the serial data input for the device. This signal is sent from the host (master) to the device (slave). This signal is required to send commands to the device. Once the devices parameters such as the device key etc. have been set and saved, this signal may not be required anymore. If this signal is not used, it must be held high.
.
The DAV signal is the data available output for the device. This signal is sent from the device (slave) to the host (master). This signal is normally low. As soon as the device has something to transmit to the host, it will set this signal high. The device will keep this signal high until the host clocks in the last bit of the last byte that the device wants to transmit to the host. At this point, the device will set this signal low. The host can use this signal to determine if the device has data ready to transmit such as card data or a command response. Optionally, this signal can be left open, however, the host would then need to poll the device periodically to determine if it has data to transmit. This is explained further in the communications protocol section of this document. Immediately after the device is power cycled or reset this signal is in an indeterminate state for a maximum of 1 second. This signal should be ignored during this time.

The CS/ signal is the chip select input for the device. This signal is sent from the host (master) to the device (slave). When this signal is high, the device will ignore the SCL and SDI signals. When this signal is low the device will respond to the SCL and SDI signals. This signal can be used by hosts that have more than one slave attached to the SPI bus to control which slave the host wants to communicate with. If the host does not need to use this signal, it should be connected to ground. The CS/ signal must be low for at least 1us before the active edge of SCL for each byte transfer.

The VIN signal is the power input for the device. This signal has an operating range of 2.7 to 3.6 volts DC.

The GND signal is logic ground.

The head case GND signal is frame ground. It is connected to the head case. For optimum ESD protection, this signal should be connected to earth ground.

COMMUNICATION PROTOCOL

The Encrypting SPI IntelliHead supports full duplex communication.

<IDLE> is the idle character. The <IDLE> character is 0xFF. By definition, SPI requires that the host clocks a byte in from the device every time the host clocks a byte out to the device. Since the device will not always have a frame to send to the host every time the host has a frame to send to the device and vice versa, the idle character will always be sent by either the host or the device when it is not transmitting a frame. Note that the contents of some frame fields could have bytes with the value 0xFF. These bytes should not be mistaken for <IDLE> characters.

Frames are formatted as follows:

<SOF><LENH><LENL><MSG DATA>

All fields are required.

<SOF> is the start of frame character. The <SOF> character is 0x01. This character is used to signal that the bus is no longer in the <IDLE> condition and that a frame is starting.

<LENH> is the high byte of the two-byte length field. The length field indicates how many bytes are contained in the <MSG DATA> field. Most <MSG DATA> fields contain fewer than 256 bytes so this field is usually set to zero.

<LENL> is the low byte of the two byte length field. The length field indicates how many bytes are contained in the <MSG DATA> field.

<MSG DATA> is the message data field. The number of bytes contained in this field is specified by the two byte length field.

Frames are formatted the same for the host-to-device and the device-to-host directions. When the host has a frame to send, it simply clocks it out. When the device has a frame to send it raises its data available (DAV) signal and waits for the host to clock in the frame. The host normally clocks out <IDLE> characters to clock in a frame from the device. Since the device typically loads its two transmit buffers with <IDLE> bytes when it has nothing to transmit, the first 2 bytes clocked out from the device after the DAV signal is asserted could be <IDLE> bytes instead of a <SOF> byte. If this is the case, simply discard these bytes. To detect when the device has a frame to send, the host can either monitor the DAV signal or, optionally, periodically clock in up to three bytes from the device to see if the device has sent a <SOF>. Up to three bytes should be clocked in instead of just one because the first two bytes could be <IDLE> bytes that were loaded into the device's transmit buffers before the device had anything to send. The host should look at each byte it clocks in to see if it is a <SOF> byte. If a <SOF> byte is found, then the subsequent bytes will contain the frame.

TIMEOUTS

The device uses a clock character timeout (CCT) to recover from the possible error condition in which the host starts to clock a character but the entire character is not clocked. The CCT defaults to 2 seconds; however, it can be adjusted. Once the host clocks the first bit of a character, the CCT timer starts running. If the timer expires before the host clocks the eighth bit of the character, the device will reset its SPI communications engine to the state it is in after a power cycle or reset. Any frames that were being received or transmitted will be lost. This includes frames containing card data. At this point the device will be ready to receive or transmit new frames.

The device uses a receive inter character timeout (RICT) to recover from the possible error condition in which the device starts to receive a frame but the entire frame is not received. The RICT defaults to 2 seconds; however, it can be adjusted. Once the device receives a <SOF> character the RICT timer starts running. It is reset each time the device receives another character of the frame. If the timer expires before the last byte of the frame is received, the device will reset its SPI communications engine to the state it is in after a power cycle or reset. Any frames that were being received or transmitted will be lost. This includes frames containing card data. At this point, the device will be ready to receive or transmit new frames.

The device uses a data available timeout (DAVT) to recover from the possible error condition in which the device asserts the data available signal but no <SOF> character is transmitted. The DAVT defaults to 0 (disabled), however, it can be adjusted. Once the DAV signal is asserted, the DAVT timer starts running. If the timer expires before a <SOF> character is transmitted, the device will reset its SPI communications engine to the state it is in after a power cycle or reset. Any frames that were being received or transmitted will be lost. This includes frames containing card data. At this point, the device will be ready to receive or transmit new frames. Note that the timer will be reset each time the device transmits an <IDLE> character after asserting the DAV signal and prior to transmitting the <SOF> character.

The device uses a transmit inter character timeout (TICT) to recover from the possible error condition in which the device starts to transmit a frame but the entire frame is not transmitted. The TICT defaults to 2 seconds; however, it can be adjusted. Once the DAV signal is asserted and the device transmits a <SOF> character, the TICT timer starts running. It is reset each time the device transmits another character. If the timer expires before the last byte of the frame is transmitted, the device will reset its SPI communications engine to the state it is in after a power cycle or reset. Any frames that were being received or transmitted will be lost. This includes frames containing card data. At this point the device will be ready to receive or transmit new frames.

MESSAGE DATA

<MTYP> is the message type field. This is always the first byte of the <MSG DATA> field. The value of this field determines what type of message is being sent. The following table defines the valid values of the <MTYP> field.

<MTYP> Value	Description
0x00	Request message
0x01	Response message
0x02	Notification message

Request Message

The Request Message is used to send a command request from the host to the device. The <MSG DATA> field of this type of message is structured as follows:

<MTYP><CMD><REQ DATA>

<CMD> is the command identifier. This one byte field is used to uniquely identify the command.

<REQ DATA> is the request data field. The value and length of this field is dependent on the command.

Response Message

The Response Message is used to send command responses from the device to the host. The device will respond to request messages with a response message. The device can only process one request message at a time. Once the host sends a request message to the device, the host should wait for the response message before sending another request message. The <MSG DATA> field of this type of message is structured as follows:

<MTYP><RC><RSP DATA>

<RC> is the result code. The result code is a one byte field that contains a value that can be used to determine if the command succeeded or not.

There are two types of result codes: generic result codes and command-specific result codes. Generic result codes always have the most significant bit set to zero. Generic result codes have the same meaning for all commands and can be used by any command. Command-specific result codes always have the most significant bit set to one. Command-specific result codes are defined by the command that uses them. The same result code can have different meanings for different commands. Command-specific result codes are defined in the documentation for the command that uses them. Generic Result codes are defined in the following table.

Generic Result Code Table

Value	Result Code	Description
0	SUCCESS	The command completed successfully.
1	FAILURE	The command failed.
2	BAD_PARAMETER	The command failed due to a bad parameter or command syntax error.

<RSP DATA> is the response data field. The value and length of this field is dependent on the command.

Notification Message

The Notification Message is used to send unsolicited messages from the device to the host. This type of message is typically used to send card data to the host. The <MSG DATA> field of this type of message is structured as follows:

<MTYP><NID><NTN DATA>

<NID> is the notification identifier. This one byte field is used to uniquely identify the notification message.

<NTN DATA> is the notification data field. The value and length of this field is dependent on the notification identifier.

CARD DATA NOTIFICATION MESSAGE

After a card swipe in either the forward or reverse direction, the data is encrypted and the DAV line is asserted. When the host begins clocking, the reader will transmit data in the following order:

[***<SOF><LEN><MTYP><NID>***] [***Device Serial Number***] [***Card data from Delta ASIC***]

Where:

<SOF> is 0x01

<LEN> is 0x01 0x1A (282 bytes)

<MTYP> is 0x02

<NID> is 0x00

Device Serial Number is the clear text binary 8-byte value that can be TDEA encrypted under the Base Derivation Key by the Host to determine the Device Key. (See Appendix C. Derivation Of The Device Key for information on how the Device Key can be derived by using the device serial number in combination with the base derivation key.) (See the Device Serial Number Property section for information on how the device serial number can be get, set and saved.)

Card data from Delta ASIC consists of 6 random bytes plus the 2 bytes of the Delta ASIC header followed by all 2112 binary bits (264 bytes) from the Delta ASIC. This data is not decoded or formatted. It consists of the raw bits from each track of card data. This data consists of 88 bytes for each of three tracks. Track 1 is first followed by track 2 then 3. If the track is blank it will consist of all zeros. The first byte of each track is the first byte read by the head. The least significant bit of each byte is the first bit read by the head. Data starts being collected when the first 1 bit is detected. So if the first character read by the head is the LRC any leading zeros of the LRC will not be included in the track data so this must be considered when decoding the track data. For more details about the track data see the Delta ASIC specification. If the Encrypt Card Data property is set to true, all bytes in this field are TDEA encrypted under the Device Key using the CBC method. If the Encrypt Card Data property is set to false, this field is not encrypted. (See appendix B. Guide To Decrypting Data)

SECTION 3. OPERATION COMMANDS

GET AND SET PROPERTY COMMANDS

The **Get Property** command gets a property from the device. The **Get Property** command number is 0.

The **Set Property** command sets a property in the device. The **Set Property** command number is 1.

The Get and Set Property request and response data fields are structured as follows:

Get Property Request Data:

Data Offset	Value
0	Property ID

Get Property Response Data:

Data Offset	Value
0 – n	Property Value

Set Property Request Data:

Data Offset	Value
0	Property ID
1 – n	Property Value

Set Property Response Data: None

The result codes for the Get and Set Property commands can be any of the codes listed in the **Generic Result Code Table**.

Property ID is a one-byte field that contains a value that identifies the property.

The **Property Value** is a multi-byte field that contains the value of the property. The number of bytes in this field depends on the property.

SOFTWARE ID PROPERTY

Property ID: 0
Value length: 11 bytes
Get Property: Yes
Set Property: No

Description: This is the 11-byte read-only property that identifies the software part number and version for the device. The first 8 bytes represent the part number and the last 3 bytes represent the version. For example this string might be "21088853A02". This string is subject to change. Examples follow:

Example Get Software_ID property Request (Hex):

SOF	LEN	MTYP	CMD	PID
01	00 03	00	00	00

Example Get SOFTWARE_ID property Response (Hex):

SOF	LEN	MTYP	RC	PVAL
01	00 0D	01	00	32 31 30 38 38 38 35 33 41 30 32

DEVICE SERIAL NUMBER PROPERTY

Property ID: 1
Value length: 8 bytes
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: (Hex) 00 00 00 00 00 00 00 00

Description: This property contains the eight byte device serial number. This device serial number is sent to the host in the **Card Data Notification Message**. (See the card data notification message data format section for more information.)

Changes made to the value of this property will be effective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Device_Serial_Number property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 0B	00	01	01	31 32 33 34 35 36 37 38

Example Set Device_Serial_Number property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

ENCRYPT CARD DATA PROPERTY

Property ID: 2
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 0 (false)

Description: When this property is set to 1 (true), the card data field in the card data notification message is encrypted. If this property is set to 0 (false), the card data field is not encrypted.

If this property is set to true and an attempt is made to set it to false, this attempt will fail unless the **External Authenticate Command** is successfully issued first. So it is very important that the device key be known before setting this property to true or else this property can never be set back to false and card data cannot be decrypted. When this is the case, the device is essentially useless.

Changes made to the value of this property will be effective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Encrypt_Card_Data property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	02	01

Example Set Encrypt_Card_Data property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

LOCK DEVICE KEY PROPERTY

Property ID: 3
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 0 (false)

Description: When this property is set to 1 (true), the device key can no longer be changed unless the **External Authenticate Command** is successfully issued first. If this property is set to 0 (false), the device key can be changed.

If this property is set to true and an attempt is made to set it to false, this attempt will fail unless the **External Authenticate Command** is successfully issued first. So it is very important that the device key be known before setting this property to true or else this property can never be set back to false and card data cannot be decrypted. When this is the case, the device is essentially useless.

Changes made to the value of this property will be affective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Lock_Device_Key property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	03	01

Example Set Lock_Device_Key property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

ENCRYPTED CHALLENGE PROPERTY

Property ID: 4
Value length: 8 bytes
Get Property: Yes
Set Property: No

Description: This property contains 8 bytes of encrypted random data. This data will vary each time it is retrieved. This data is used with the **External Authenticate Command.**

Example Get Encrypted_Challenge property Request (Hex):

SOF	LEN	MTYP	CMD	PID
01	00 03	00	00	04

Example Get Encrypted_Challenge property Response (Hex):

SOF	LEN	MTYP	RC	PVAL
01	00 0A	01	00	45 86 F5 14 A5 12 8C BE

RECEIVE INTER CHARACTER TIMEOUT PROPERTY

Property ID: 5
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 20 (2 seconds)

Description: This property can be used to adjust or disable the receive inter character timeout. This property can have a value of 0 – 250. When set to 0, the timeout is disabled. When set between 1 and 250, the timeout is equal to the value of this property multiplied by 100ms. For example, if the value is set to 20, the timeout would be equal to 20 times 100ms which equals 2000ms (2 seconds). See the Timeouts section of this manual for a description of how this timeout works.

Changes made to the value of this property will be effective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Receive_Inter_Character_Timeout property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	05	20

Example Set Receive_Inter_Character_Timeout property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

DATA AVAILABLE TIMEOUT PROPERTY

Property ID: 6
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 0 (disabled)

Description: This property can be used to adjust or disable the data available timeout. This property can have a value of 0 – 250. When set to 0, the timeout is disabled. When set between 1 and 250, the timeout is equal to the value of this property multiplied by 100ms. For example, if the value is set to 20, the timeout would be equal to 20 times 100ms which equals 2000ms (2 seconds). See the timeouts section of this manual for a complete description of how this timeout works. See the Timeouts section of this manual for a description of how this timeout works.

Changes made to the value of this property will be effective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Data_Available_Timeout property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	06	20

Example Set Data_Available_Timeout property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

TRANSMIT INTER CHARACTER TIMEOUT PROPERTY

Property ID: 7
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 20 (2 seconds)

Description: This property can be used to adjust or disable the *transmit inter character timeout*. This property can have a value of 0 – 250. When set to 0, the timeout is disabled. When set between 1 and 250, the timeout is equal to the value of this property multiplied by 100ms. For example, if the value is set to 20, the timeout would be equal to 20 times 100ms which equals 2000ms (2 seconds). See the Timeouts section of this manual for a description of how this timeout works.

Changes made to the value of this property will be effective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Transmit Inter Character Timeout property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	07	20

Example Set Transmit Inter Character Timeout property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

SPI CLOCK PHASE AND POLARITY PROPERTY

Property ID: 8
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 0 (Clock Phase = 0, Clock Polarity = 0)

Description: This property can be used to adjust the SPI clock phase and polarity. Both the host and the device must be set to the same SPI clock phase and polarity in order to communicate correctly. This property can have a value in the range of 0 to 3. The following table shows how each value should be interpreted.

Value	Clock Phase	Clock Polarity	Description
0	0	0	Data centered on first edge of clock period. Clock line low in idle state.
1	0	1	Data centered on first edge of clock period. Clock line high in idle state.
2	1	0	Data centered on second edge of clock period. Clock line low in idle state.
3	1	1	Data centered on second edge of clock period. Clock line high in idle state.

Changes made to the value of this property will not take effect until after the device is power cycled or reset. These changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set SPI_Clock_Phase_and_Polarity property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	08	00

Example Set SPI_Clock_Phase_and_Polarity property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

CLOCK CHARACTER TIMEOUT PROPERTY

Property ID: 9
Value length: 1 byte
Get Property: Yes
Set Property: Yes
Non-volatile: Yes
Default value: 20 (2 seconds)

Description: This property can be used to adjust or disable the clock character timeout. This property can have a value of 0 – 250. When set to 0, the timeout is disabled. When set between 1 and 250, the timeout is equal to the value of this property multiplied by 100ms. For example, if the value is set to 20, the timeout would be equal to 20 times 100ms which equals 2000ms (2 seconds). See the Timeouts section of this manual for a description of how this timeout works.

Changes made to the value of this property will be effective immediately; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing this property.

Example Set Clock Character_Timeout property Request (Hex):

SOF	LEN	MTYP	CMD	PID	PVAL
01	00 04	00	01	09	20

Example Set Clock Character_Timeout property Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

KEY CHECK VALUE PROPERTY

Property ID: 10 (0x0A)
Value length: 2 bytes
Get Property: Yes
Set Property: No

Description: This property contains a 2 byte key check value (KCV). This key check value can be used by the host to help verify that the device contains the proper key. The device derives this property by first TDEA encrypting under the device key an eight byte data field that contains all zeros. The KCV property is the first two bytes of this 8 byte encrypted data field.

Example Get Key Check Value property Request (Hex):

SOF	LEN	MTYP	CMD	PID
01	00 03	00	00	0a

Example Get Key Check Value property Response (Hex):

SOF	LEN	MTYP	RC	PVAL
01	00 04	01	00	82 43

SAVE NON-VOLATILE DATA COMMAND

Command number: 2
Description: This command is used to save certain device data that was modified with the set property command or other commands into non-volatile memory so that these modifications will still be in place after the device is power cycled or reset.

Data structure: No data is sent with this command.

Result codes: Any of the codes listed in the **Generic Result Code Table**.

Example Request (Hex):

SOF	LEN	MTYP	CMD
01	00 02	00	02

Example Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

RESET DEVICE COMMAND

Command number: 3
Description: This command is used to reset the device. After the host sends this command to the device, the host should first wait for the response from the device and then wait 5 seconds before trying to communicate further with the device so that the device has time to reset and reboot.

Data structure: No data is sent with this command.

Result codes: Any of the codes listed in the **Generic Result Code Table**.

Example Request (Hex):

SOF	LEN	MTYP	CMD
01	00 02	00	03

Example Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

LOAD DEVICE KEY COMMAND

This command should only be used in a secure environment.

Command number: 4

Description: This command loads the sixteen byte device key. This device key is used to encrypt the card data sent to the host in the **Card Data Notification Message**. (See Appendix C. Derivation Of The Device Key for information on how the Device Key can be derived by using the device serial number in combination with the base derivation key.)

The sixteen byte device key is used to perform triple DES encryption. By definition, if the first 8 bytes of the key equals the second 8 bytes of the key triple DES encryption simplifies to the less secure single DES encryption. When this is the case, this device will perform encryption three times faster than it will for triple DES. So, one can optionally use single DES encryption to speed up the device's encryption time by making the first 8 bytes of the key equal to the second 8 bytes of the key.

The **Lock Device Key Property** must be false prior to issuing this command or else the **Load Device Key Command** will fail. The **Lock Device Key Property** can be set to true after loading the device key; this will make sure that the device key can no longer be changed without knowing the current device key.

In order to increase security during the key loading process, the device key is loaded as two components. First, the host must send the **Load Device Key Command** with the **first** component. Second, the host must send the **Load Device Key Command** with the **second** component within 2 minutes of sending the first component. After the second component has been received, the two components will be XORed together to form the active device key.

The default value of the device key in hex is 0000 0000 0000 0000 0000 0000 0000 0000.

Changes made to the value of the device key will be effective immediately after the second component has been received; however, these changes will be lost after a device power cycle or reset unless the **Save Non-volatile Data Command** is also issued after changing the device key. In this case the device will revert back to the key it was using prior to attempting to load a new one.

Data structure:

Request Data:

Offset	Field Name	Description
0	Component number	1 for the first component or 2 for the second component.
1 - 16	Component	16-byte Device key component.

Response Data: None

Result codes: Any of the codes listed in the **Generic Result Code Table**. If the second key component is sent before the first component or after the first component expires (2 minutes), the result code will indicate a failure.

The example below shows the commands that are used to load following key:

```
0011 2233 4455 6677 8899 AABB CCDD EEFF
```

The two components are

```
46EB 17C3 27D0 B6A3 9527 2152 146D 08A3
```

and

```
46FA 35F0 6385 D0D4 1DBE 8BE9 D8B0 E65C
```

Example Load Device Key command Request for the first component (Hex):

SOF	LEN	MTYP	CMD	Component Number	Component
01	00 13	00	04	01	46EB 17C3 27D0 B6A3 9527 2152 146D 08A3

Example Load Device Key command Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

Example Load Device Key command Request for the second component (Hex):

SOF	LEN	MTYP	CMD	Component Number	Component
01	00 13	00	04	02	46FA 35F0 6385 D0D4 1DBE 8BE9 D8B0 E65C

Example Load Device Key command Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

EXTERNAL AUTHENTICATE COMMAND

Command number: 5
Description: This command is used to authenticate the host to the reader. Authentication is required before the device will successfully perform certain commands. For example, this authentication is required prior to changing the **Encrypt Card Data Property** from true to false and prior to changing the **Lock Device Key Property** from true to false. Once this command succeeds, it will not need to be issued again until the device is power cycled or reset.

In order for this command to succeed, the following sequence of events must occur in the correct order.

1) The host gets 8 bytes of encrypted random data from the device by retrieving the **Encrypted Challenge Property.**
2) The host TDEA decrypts this block of encrypted random data using the current Device Key.
3) The host sends the **External Authenticate Command** along with the first 4 bytes of the decrypted random data block in the decrypted random data field. The device will compare these 4 bytes with its first 4 bytes of random data. If the data is the same, the command will succeed. If not, the command will fail. The result code will indicate if the command succeeds or fails. If this command fails, then the host must start over at step one, retrieving new encrypted random data from the device, in order for this command to succeed on the next attempt.

Request Data:

Offset	Field Name	Description
0 - 3	Decrypted Random Data	First 4 bytes of the decrypted random data block.

Response Data: None

Result codes: Any of the codes listed in the **Generic Result Code Table**.

Example **External Authenticate Command** Request (Hex):

SOF	LEN	MTYP	CMD	Random Data
01	00 06	00	05	28 6D 8F 04

Example **External Authenticate Command** Response (Hex):

SOF	LEN	MTYP	RC
01	00 02	01	00

APPENDIX A. GLOSSARY OF TERMS

Term	Description
AAMVA	American Association for Motor Vehicle Administration
ANS	American National Standards
ASIC	Application Specific Integrated Circuit
CCT	Clock Character Timeout
CMD	Command Identifier
CS/	Chip Select (negative true)
DAV	Data Available (output)
DAVT	Data Available Timeout
DES	Data Encryption Standard
ESD	Electrostatic Discharge
GND	Logic Ground
IDLE	Idle byte
ips	Inches per second
ISO	International Standards Organization
JIS	Japanese Industry Standard
LEN	Length field
LENH	Length – High byte
LENL	Length – Low byte
LSB	Least Significant Bit
mA	Milliampere
MSB	Most Significant Bit
MSG DATA	Message Data field
MTYP	Message Type
NID	Notification Identifier
NTN DATA	Notification Data field
PCI	Payment Card Industry
PID	Property ID
PVAL	Property Value
RC	Result Code
REQ DATA	Request Data field
RICT	Receive Inter Character Timeout
RSP DATA	Response Data field
SCL	Serial Clock Input
SDI	Serial Data Input
SDO	Serial Data Output
SPI	Serial Peripheral Interface
SOF	Start of Frame character
TICT	Transmit Inter Character Timeout
TDEA	Triple Data Encryption Algorithm
VDC	Volts Direct Current
VIN	Voltage input

APPENDIX B. GUIDE TO DECRYPTING DATA

The Cipher Block Chaining (CBC) method is used by the encrypting algorithm. For a description of the CBC encryption method, refer to *ANS X9.24-2004 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques.*

Here is a simplified description of the procedure used to encrypt card data in the Encrypting SPI IntelliHead.

1. A 6-byte random number is computed.
2. This random number is placed into the first 6 bytes of an 8-byte buffer.
3. The header data from the Triple-track Delta ASIC is stored in the final two bytes of the buffer.
4. This 8-byte block is TDEA encrypted under the Device Key.
5. The result of this encryption is placed into the output buffer.
6. This result is XORed with the next 8 bytes of the output from the Delta ASIC.
7. The result is TDEA encrypted under the Device Key.
8. These steps are repeated through the end of the data block.

When the host receives the data, it can decrypt the information from the beginning of the block but it must maintain both the original (encrypted) and final (clear text) buffers. If buffer space is a concern, the process can be reversed so that the decrypted value can replace the original buffer while working backwards in 8-byte blocks. Here is a description of the reverse method.

1. Start decryption on the last 8-byte block with TDEA decryption.
2. The preceding 8-byte block is then XORed with the result to obtain the clear text data for the last block.
3. Store this clear text block in the 8 bytes just decrypted.
4. Decrypt the next earlier block (N-1) with TDEA decryption.
5. Continue back at step 2 until reaching the first block.
6. The first block can skip the XOR operation (or XOR with 0x00 bytes instead).

APPENDIX C. DERIVATION OF THE DEVICE KEY

The double-length Device Key can be generated by the following process. This method is extracted from *ANS X9.24-Part 1: 2004 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques*.

1. Copy the entire key serial number right-justified into an 8-byte register. If the key serial number is fewer than 8 bytes, pad to the left with 0xFF bytes.
2. Encrypt/decrypt/encrypt these 8 bytes using the double-length Base Derivation Key (BDK), per the TECB mode of ANS X9.52-1998.
3. Use the ciphertext produced by Step 2 as the left half of the Device Key.
4. Encrypt/decrypt/encrypt the 8-byte serial number using the double-length derivation key XORed with hexadecimal C0C0 C0C0 0000 0000 C0C0 C0C0 0000 0000, per the TECB mode of ANS X9.52-1998.
5. Use the ciphertext produced by Step 4 as the right half of the Device Key.
6. After the key has been established, it must be separated into components for loading into the Encrypting SPI IntelliHead.

The base derivation key (BDK) can be defined either by MagTek or by the customer. Each device is identified by a unique device serial number (DSN). The DSN is used to derive a unique initial key by encrypting it under the BDK. Regardless of who defines the BDK, it will need to be shared between the party who injects the initial key and the host that will be used to decrypt the transactions.

APPENDIX D. DRAWINGS

This section contains the drawings showing the mechanical dimensions and wiring connections of the Encrypting SPI IntelliHead models.

The following drawings are included:

21030033	Drawing and Wiring Connections for the 90mm Butterfly Spring Model
21030034	Drawing and Wiring Connections for the 5.08mm Beam Arm Model
21030035	Drawing and Wiring Connections for the 4.05mm Beam Arm Model
21030038	Drawing and Wiring Connections for the Accordion Spring Model
21030039	Drawing and Wiring Connections for the 43mm Spring Model
21044012	43mm Rail
21045093	90mm Standard Rail
21046008	60mm Slim Profile Rail
21047023	90mm Slim Profile Rail
21052208	Mechanical Dimensions for the Accordion Spring Model
21052231	Mechanical Dimensions for the 43mm Spring Model
21052805	Mechanical Dimensions for the 90mm Butterfly Spring Model
21062370	Mechanical Dimensions for the 4.05mm Beam Arm Model
21062377	Mechanical Dimensions for the 5.08mm Beam Arm Model
21160128	IntelliStripe 60 Front & Side Bezel
21160129	IntelliStripe 60 Front Bezel
21160133	IntelliStripe 60 Side Bezel with Latch
21170011	IntelliStripe 70 Side Bezel

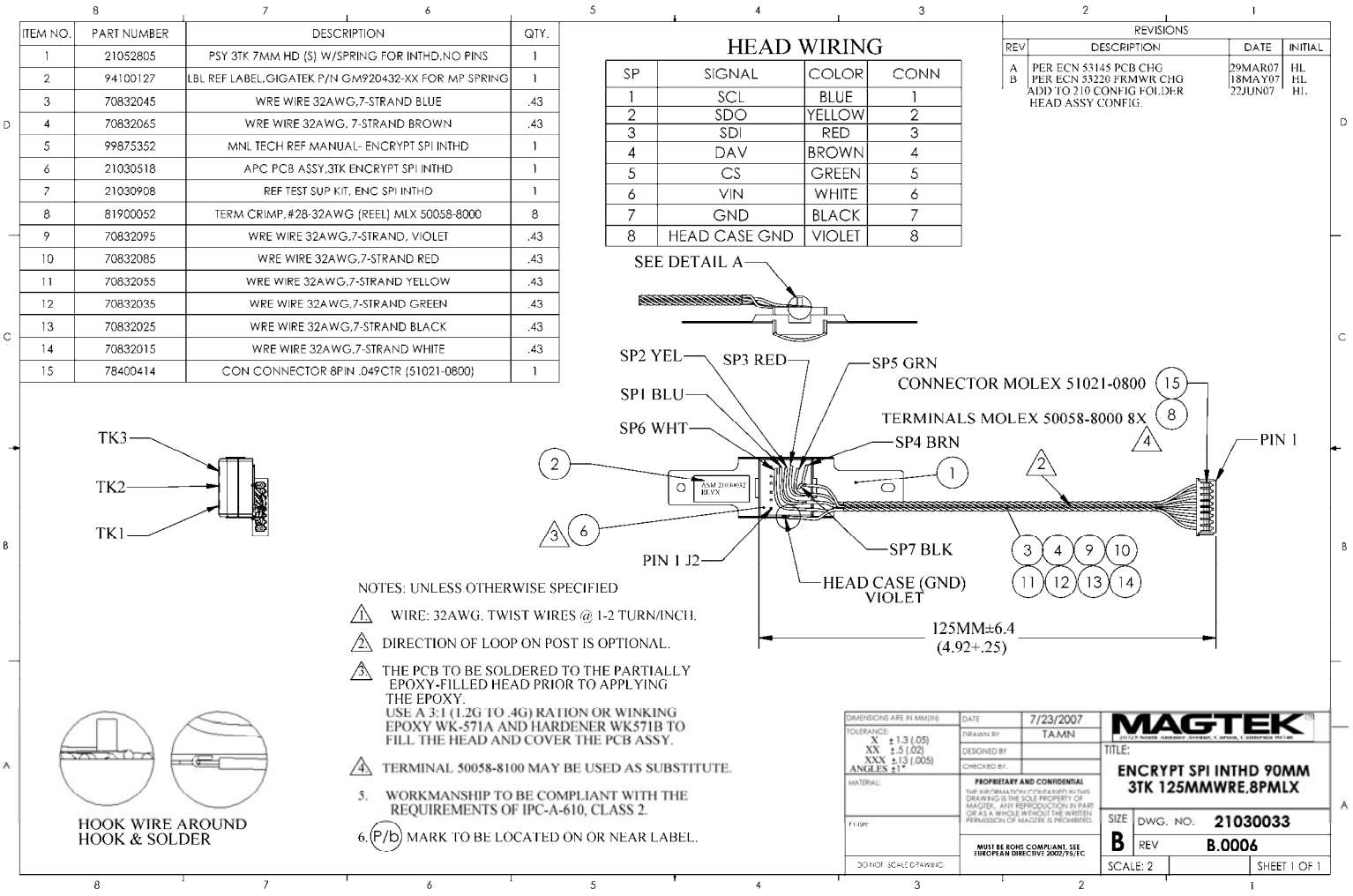


Figure C-1 90mm Butterfly Spring Model

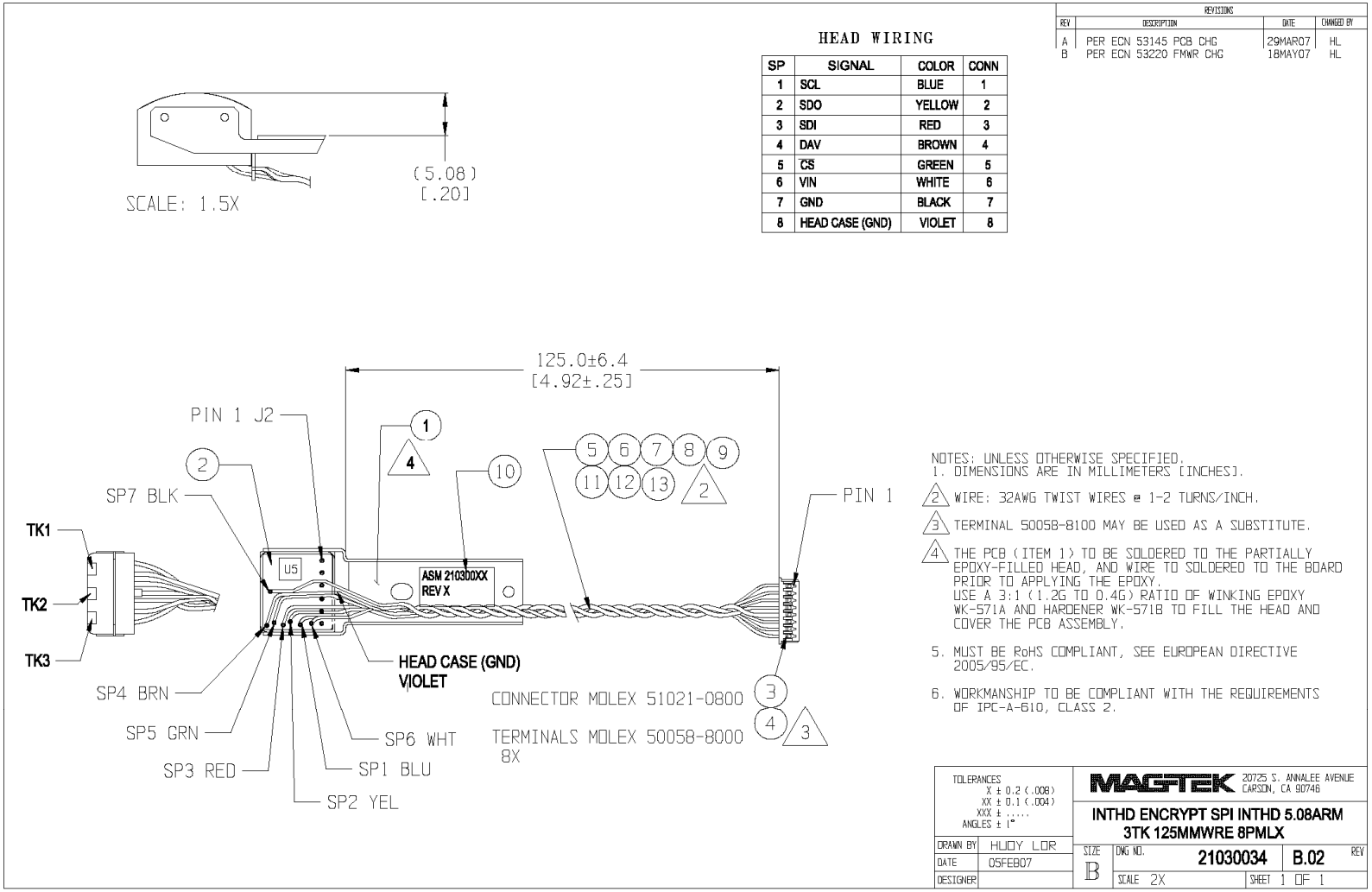


Figure C-2 5.08mm Beam Arm Model

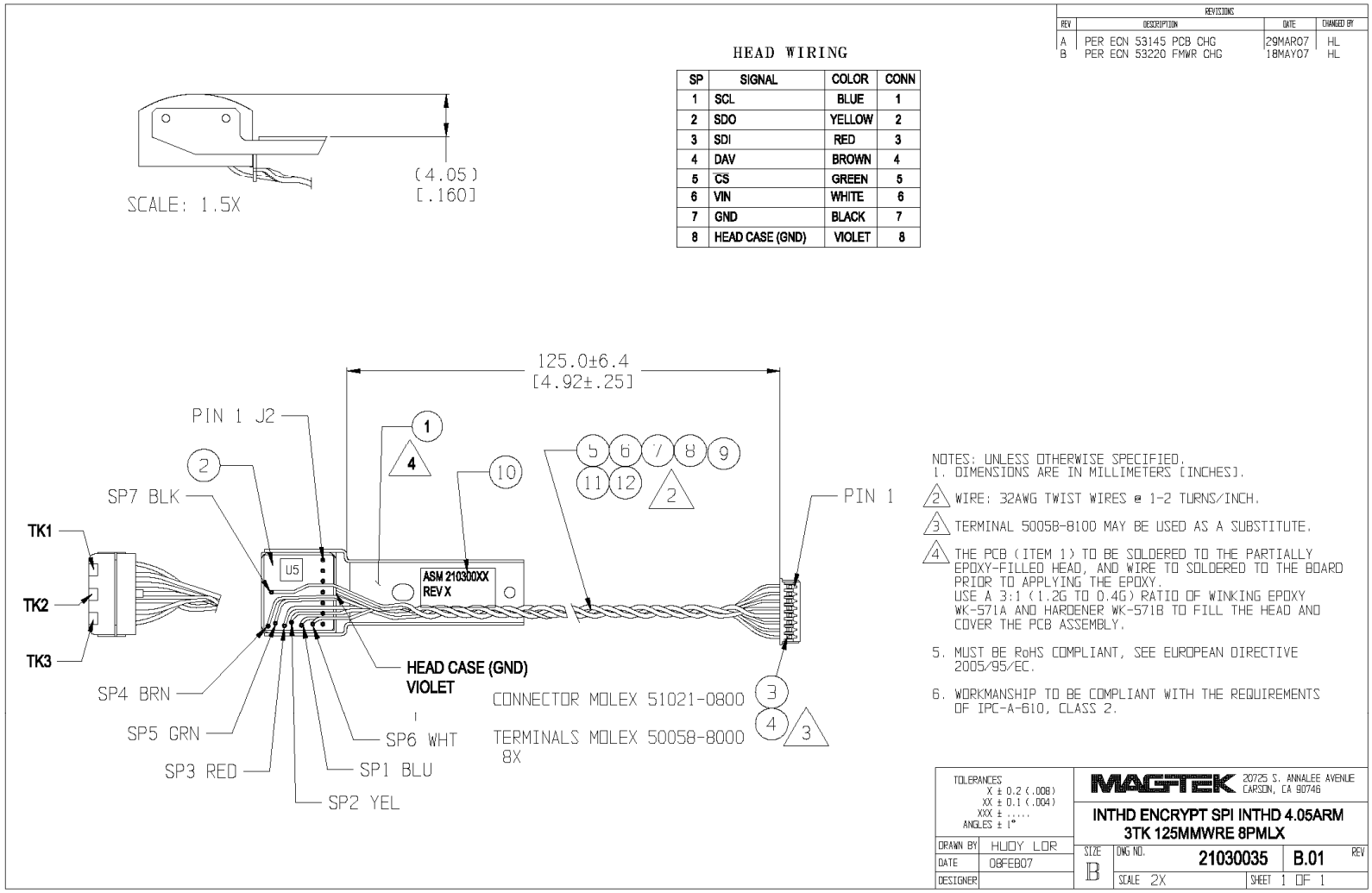


Figure C-3 4.05mm Beam Arm Model

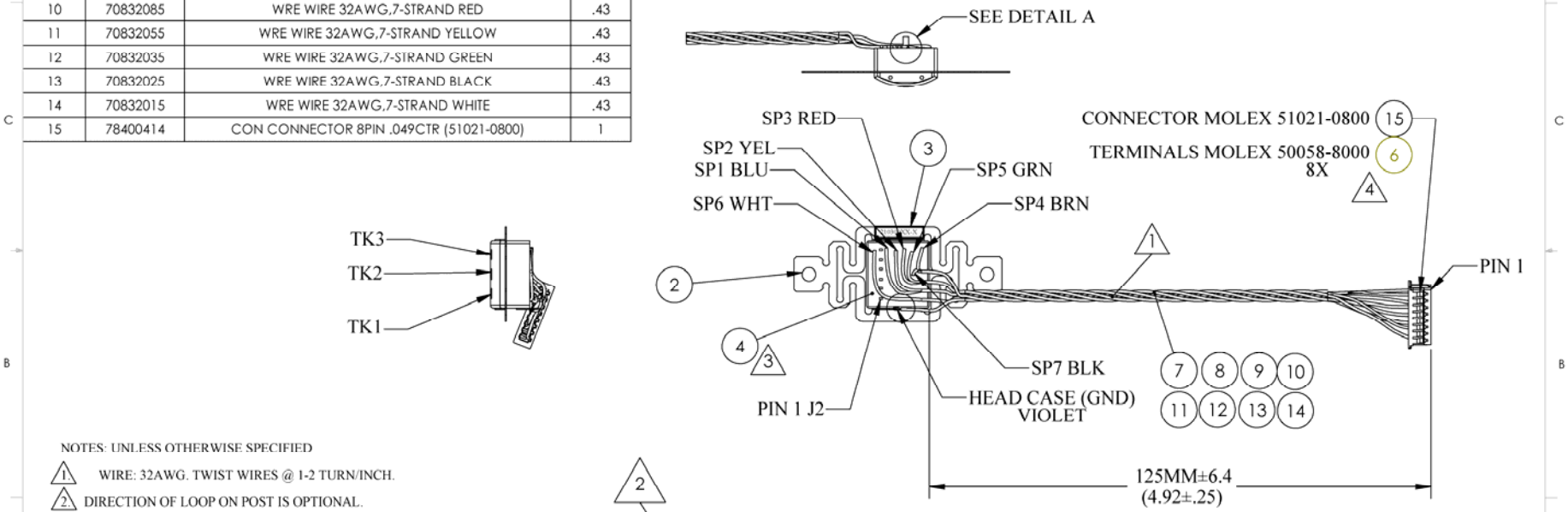
ITEM NO.	PART NUMBER	DESCRIPTION	QTY.
1	99875352	MNL TECH REF MANUAL- ENCRYPT SPI INTHD	0
2	21052208	PSY 3TK READ HD (S) 7MM/MP SPRING FOR INTHD,NO PIN	1
3	94100100	LBL REF LABEL,GIGATEK P/N GM920432-XX FOR MP SPRING	1
4	21030518	APC PCB ASSY,3TK ENCRYPT SPI INTHD	1
5	21030908	REF TEST SUP KIT, ENC SPI INTHD	1
6	81900052	TERM CRIMP,#28-32AWG (REEL) MLX 50058-8000	8
7	70832045	WRE WIRE 32AWG,7-STRAND BLUE	.43
8	70832065	WRE WIRE 32AWG, 7-STRAND BROWN	.43
9	70832095	WRE WIRE 32AWG,7-STRAND, VIOLET	.43
10	70832085	WRE WIRE 32AWG,7-STRAND RED	.43
11	70832055	WRE WIRE 32AWG,7-STRAND YELLOW	.43
12	70832035	WRE WIRE 32AWG,7-STRAND GREEN	.43
13	70832025	WRE WIRE 32AWG,7-STRAND BLACK	.43
14	70832015	WRE WIRE 32AWG,7-STRAND WHITE	.43
15	78400414	CON CONNECTOR 8PIN .049CTR (51021-0800)	1

HEAD WIRING

SP	SIGNAL	COLOR	P1, CONN
1	SCL	BLUE	1
2	SDO	YELLOW	2
3	SDI	RED	3
4	DAV	BROWN	4
5	$\overline{CS}$	GREEN	5
6	VIN	WHITE	6
7	GND	BLACK	7
8	HEAD CASE GND	VIOLET	8

REVISIONS

REV	DESCRIPTION	DATE	INITIAL
A	PER ECN 53333 PROD REL	28AUG07	HL



NOTES: UNLESS OTHERWISE SPECIFIED

1. WIRE: 32AWG. TWIST WIRES @ 1-2 TURN/INCH.
2. DIRECTION OF LOOP ON POST IS OPTIONAL.
3. THE PCB TO BE SOLDERED TO THE PARTIALLY EPOXY-FILLED HEAD PRIOR TO APPLYING THE EPOXY. USE A 3:1 (1.2G TO .4G) RATIO OR WINKING EPOXY WK-571A AND HARDENER WK571B TO FILL THE HEAD AND COVER THE PCB ASSY.
4. TERMINAL 50058-8100 MAY BE USED AS SUBSTITUTE.
5. WORKMANSHIP TO BE COMPLIANT WITH THE REQUIREMENTS OF IPC-A-610, CLASS 2.
6. P/b MARK TO BE LOCATED ON OR NEAR LABEL.

DIMENSIONS ARE IN MM[IN]
TOLERANCE: X ±1.3 (.05), XX ±.5 (.02), XXX ±.13 (.005), ANGLES ±1°
MATERIAL:
FINISH:
DO NOT SCALE DRAWING

DATE 8/29/2007
DRAWN BY H.L.
DESIGNED BY
CHECKED BY:

PROPRIETARY AND CONFIDENTIAL
THE INFORMATION CONTAINED IN THIS DRAWING IS THE SOLE PROPERTY OF MAGTEK. ANY REPRODUCTION IN PART OR AS A WHOLE WITHOUT THE WRITTEN PERMISSION OF MAGTEK IS PROHIBITED.
MUST BE ROHS COMPLIANT, SEE EUROPEAN DIRECTIVE 2002/95/EC

MAGTEK
20725 South Annalee Avenue, Carson, California 90746

TITLE: ENCRYPT SPI INTHD MP-SPR 3TK 125MMWRE, 8PMLX

SIZE B | DWG. NO. 21030038 | REV A.0002 | SCALE: 2 | SHEET 1 OF 1

Figure C-4 Accordion Spring Model

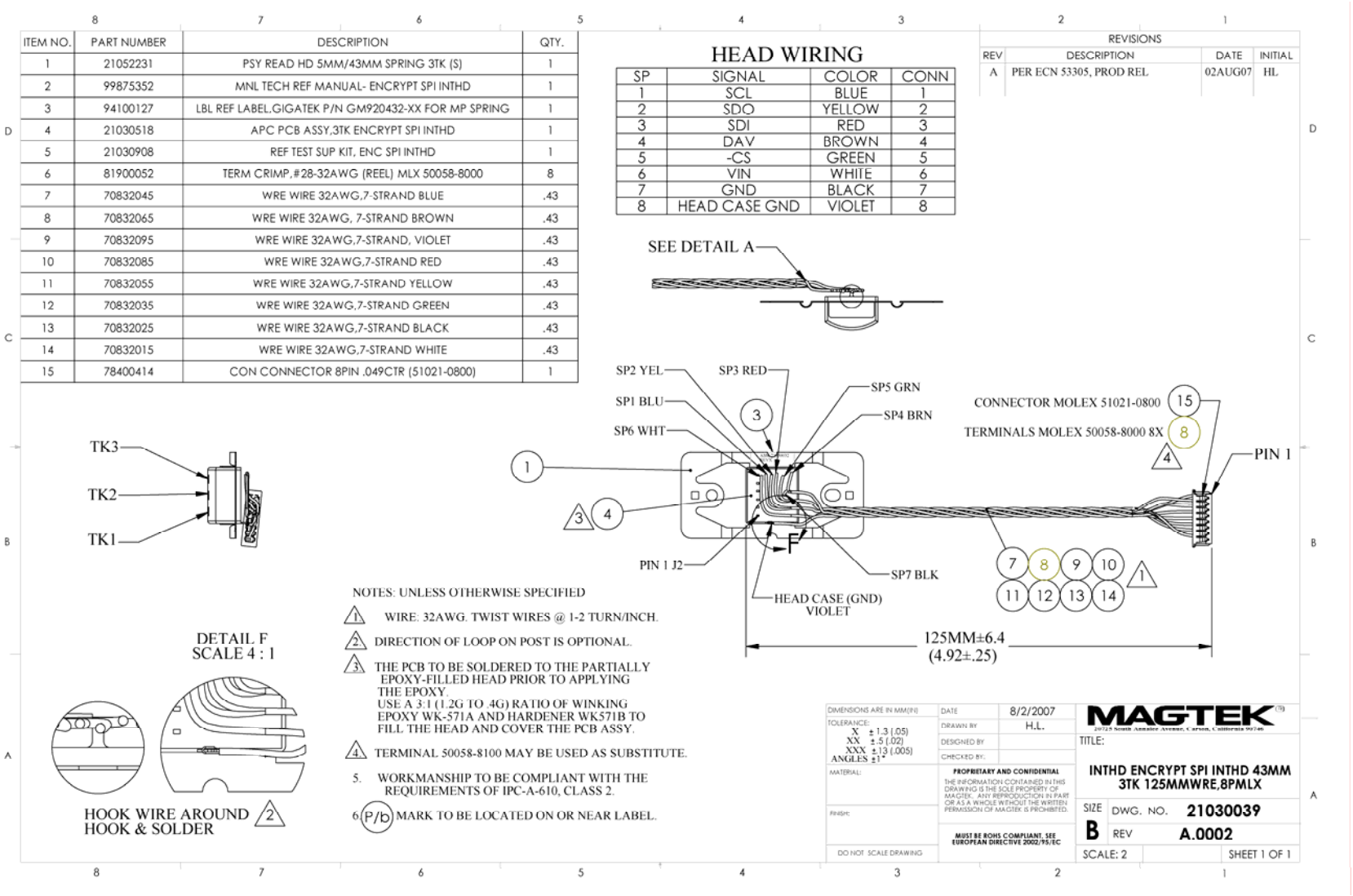


Figure C-5 43mm Spring Model

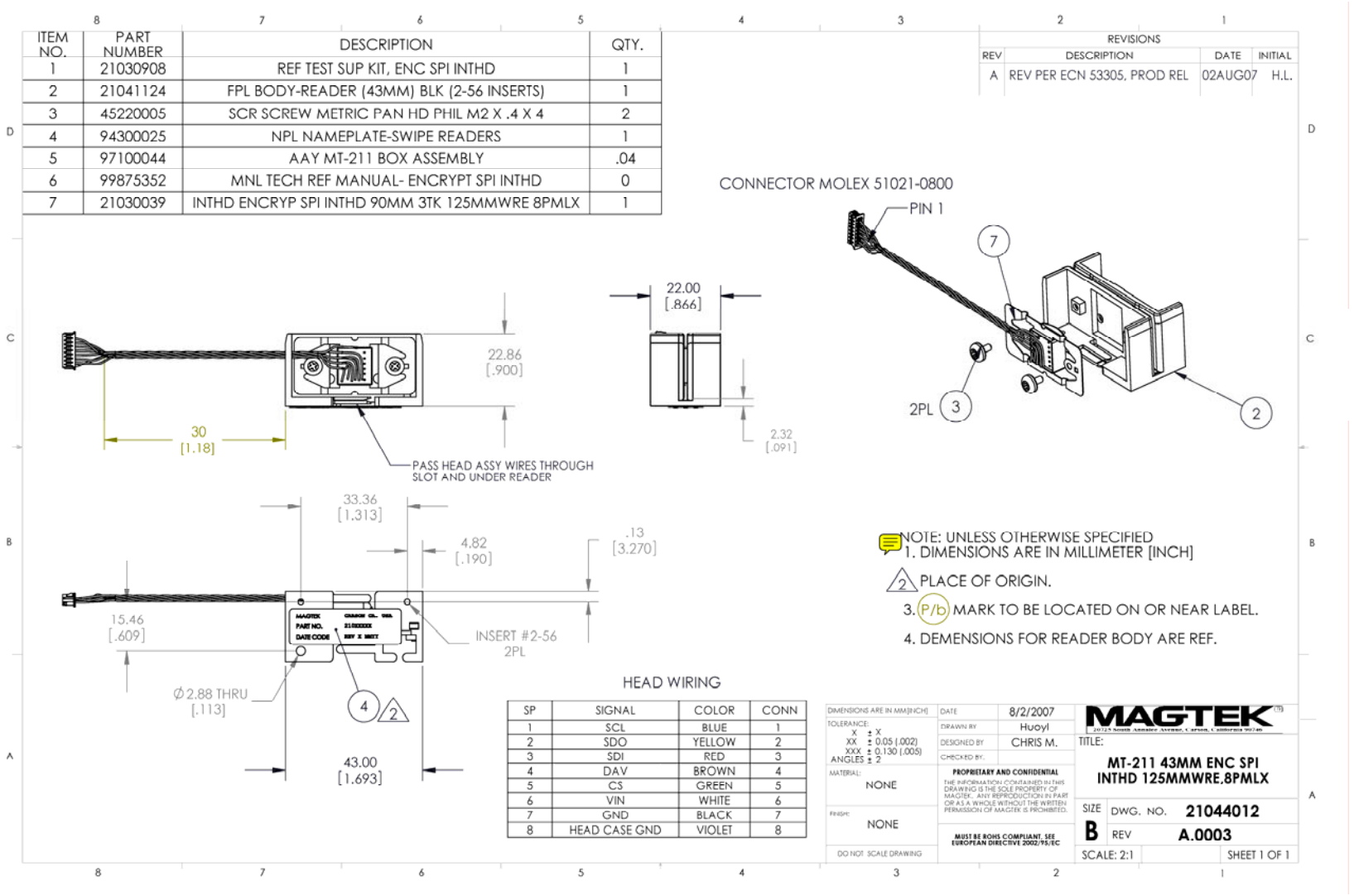


Figure C-6 43mm Rail

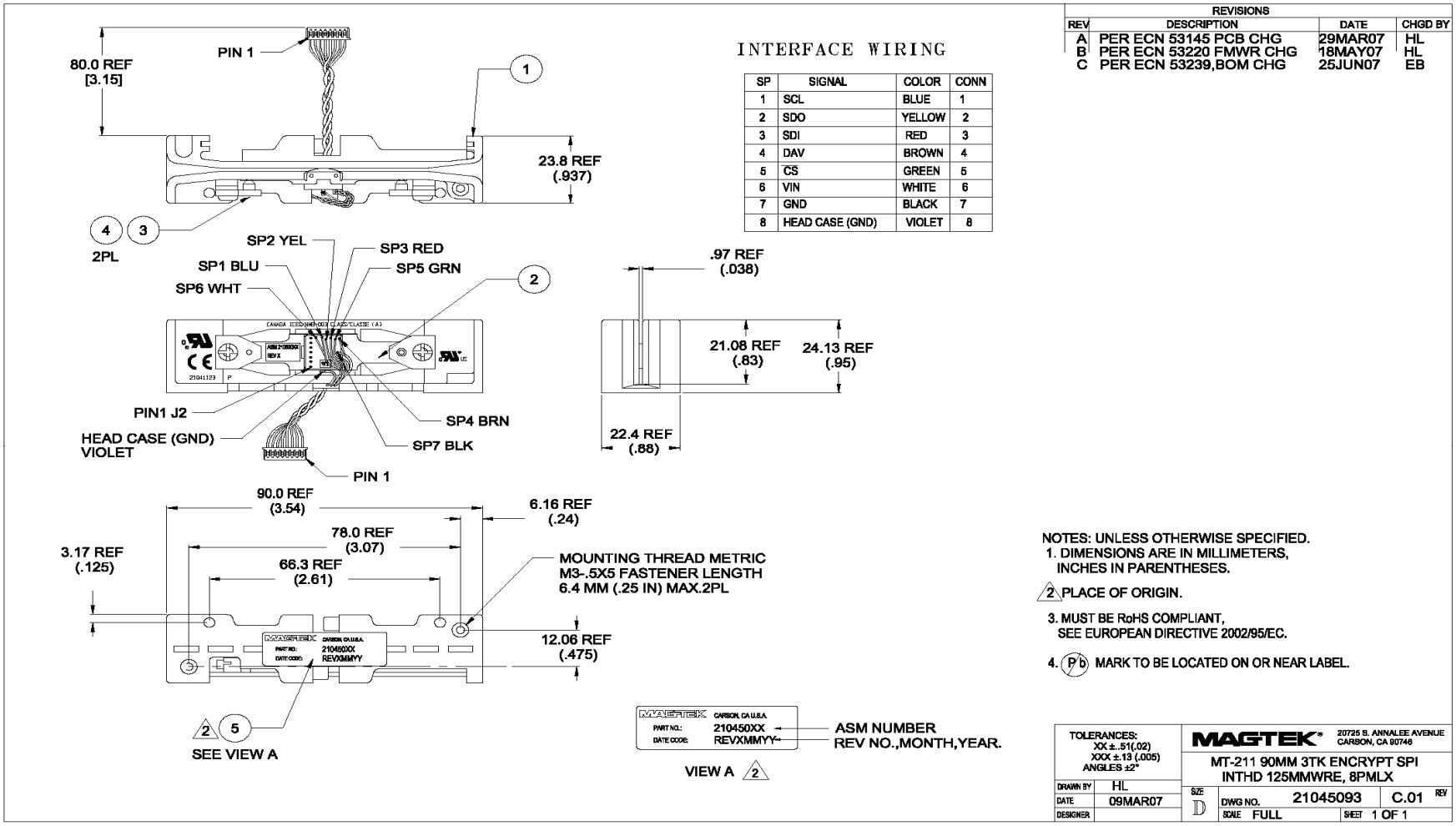


Figure C-7 90mm Standard Rail

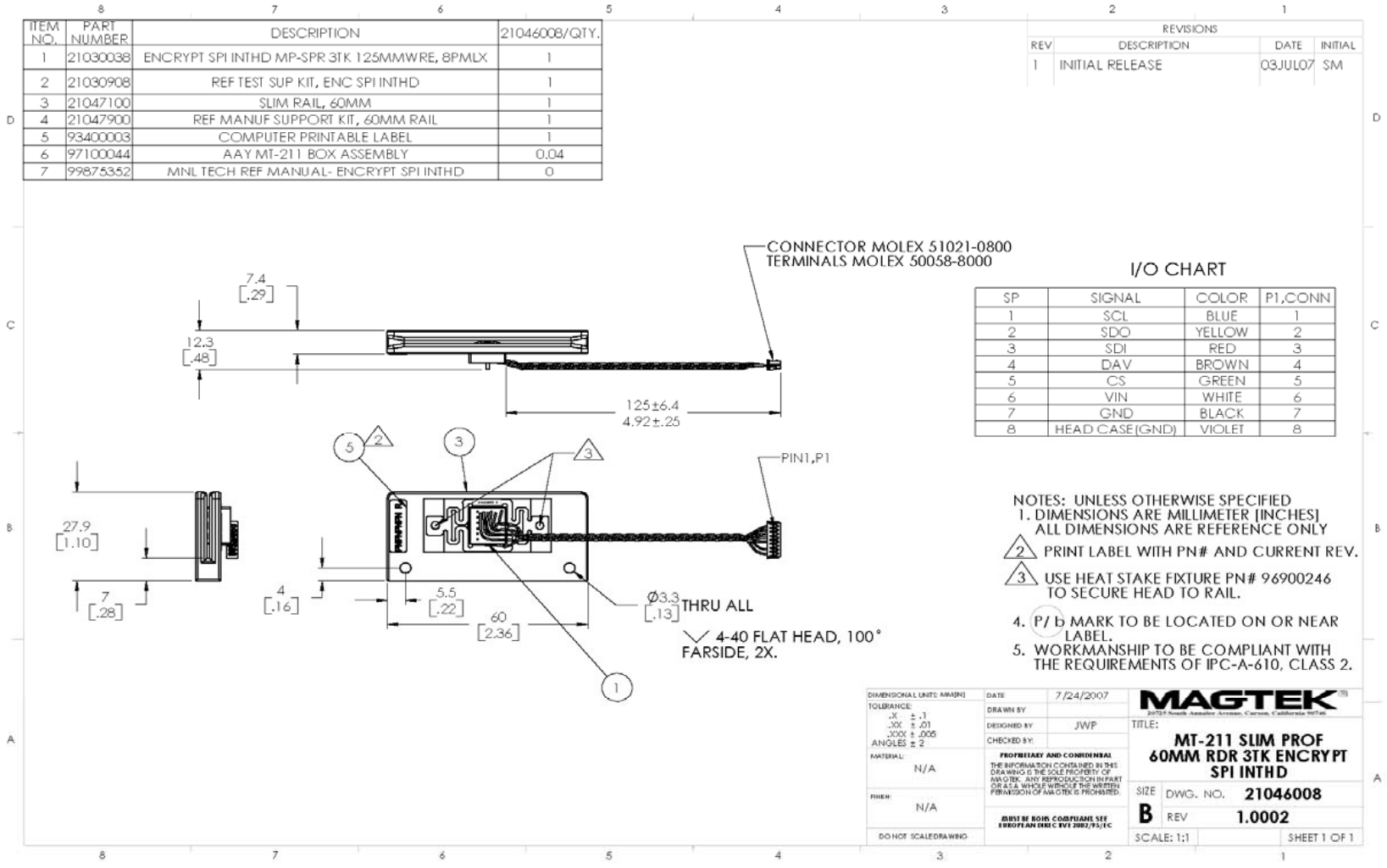


Figure C-8 60mm Slim Profile

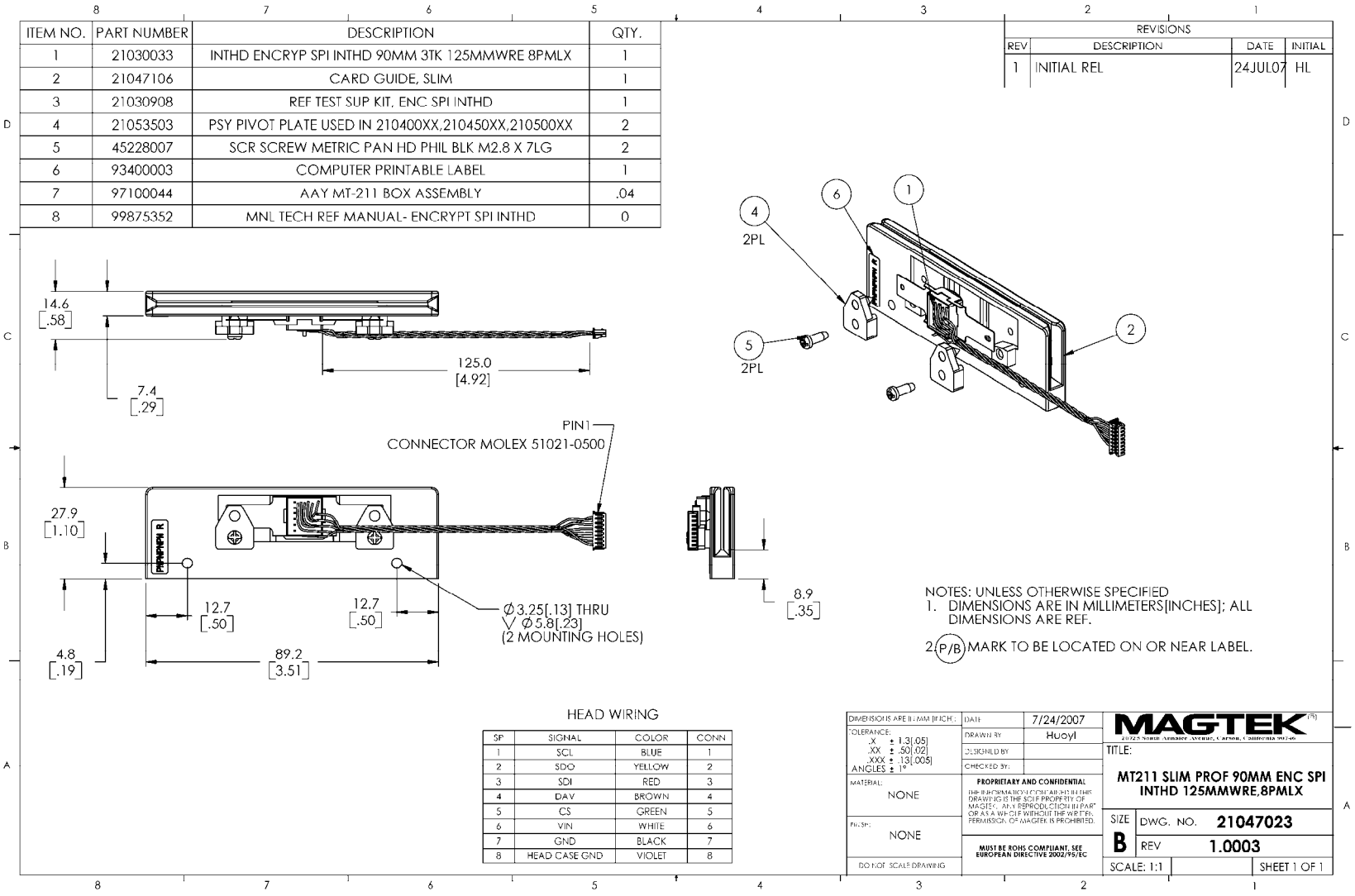


Figure C-9 90mm Slim Profile Rail

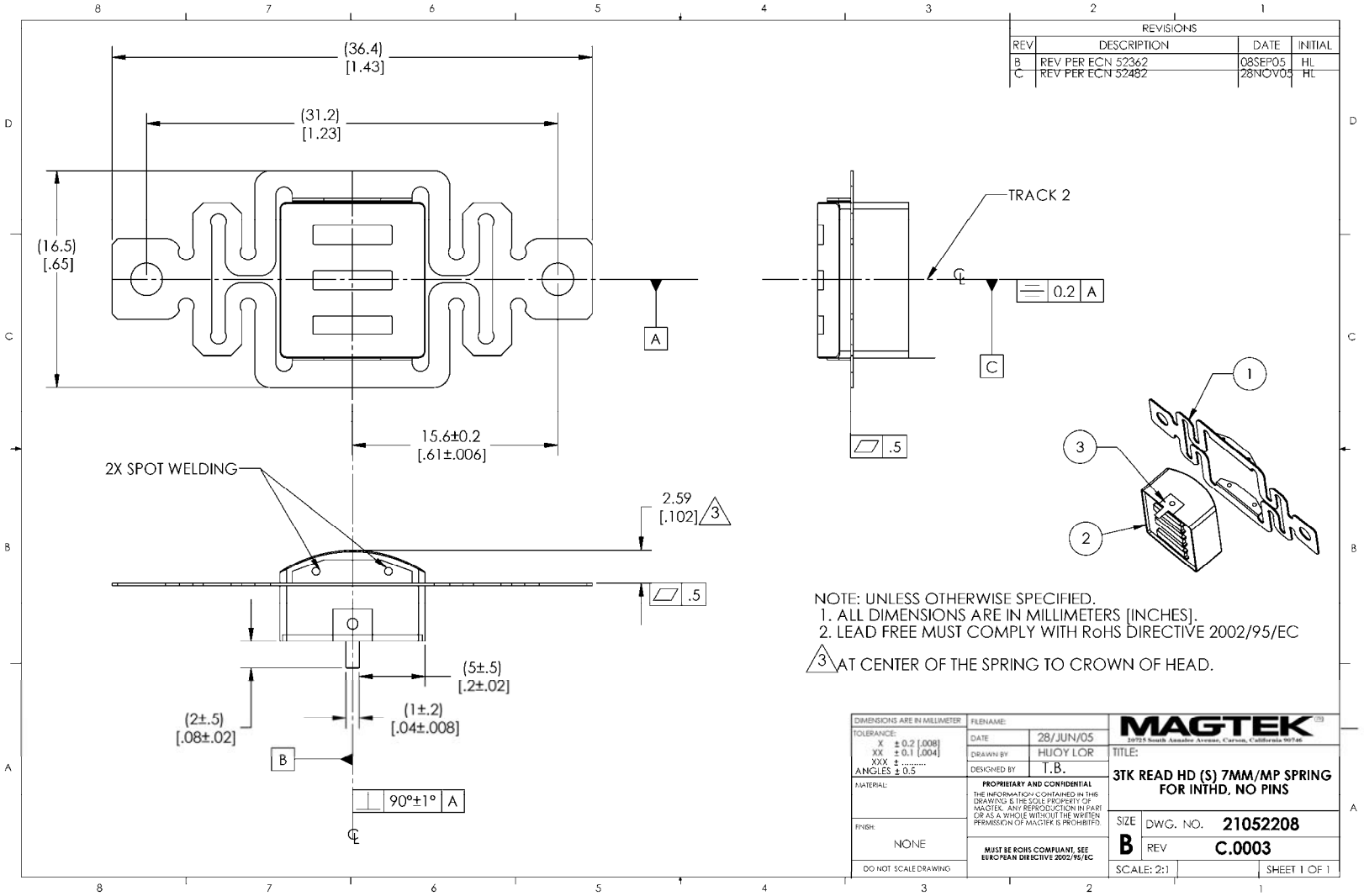


Figure C-10 Dimensions for Accordion Spring Model

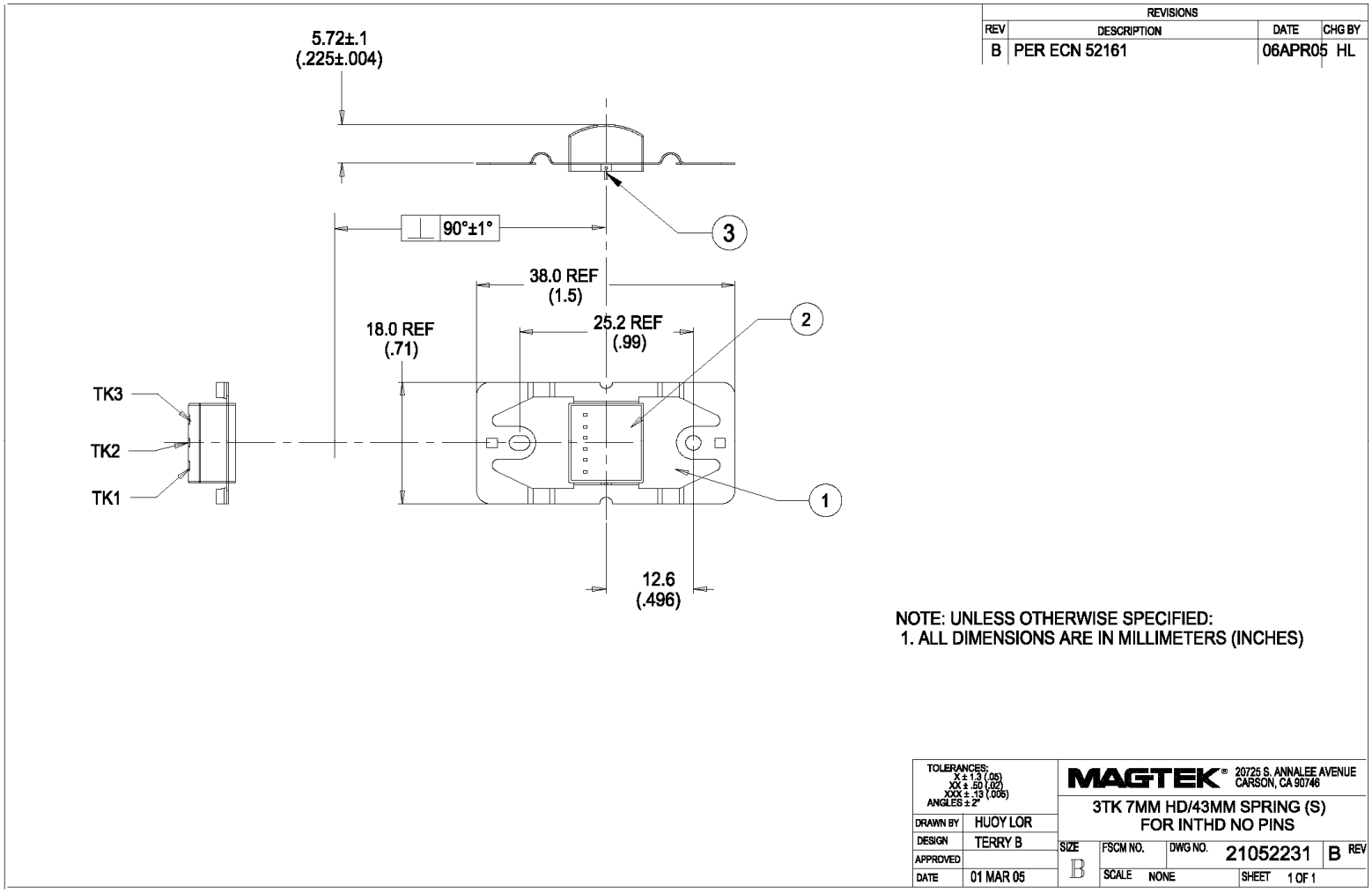


Figure C-11 Dimensions for 43mm Spring Model

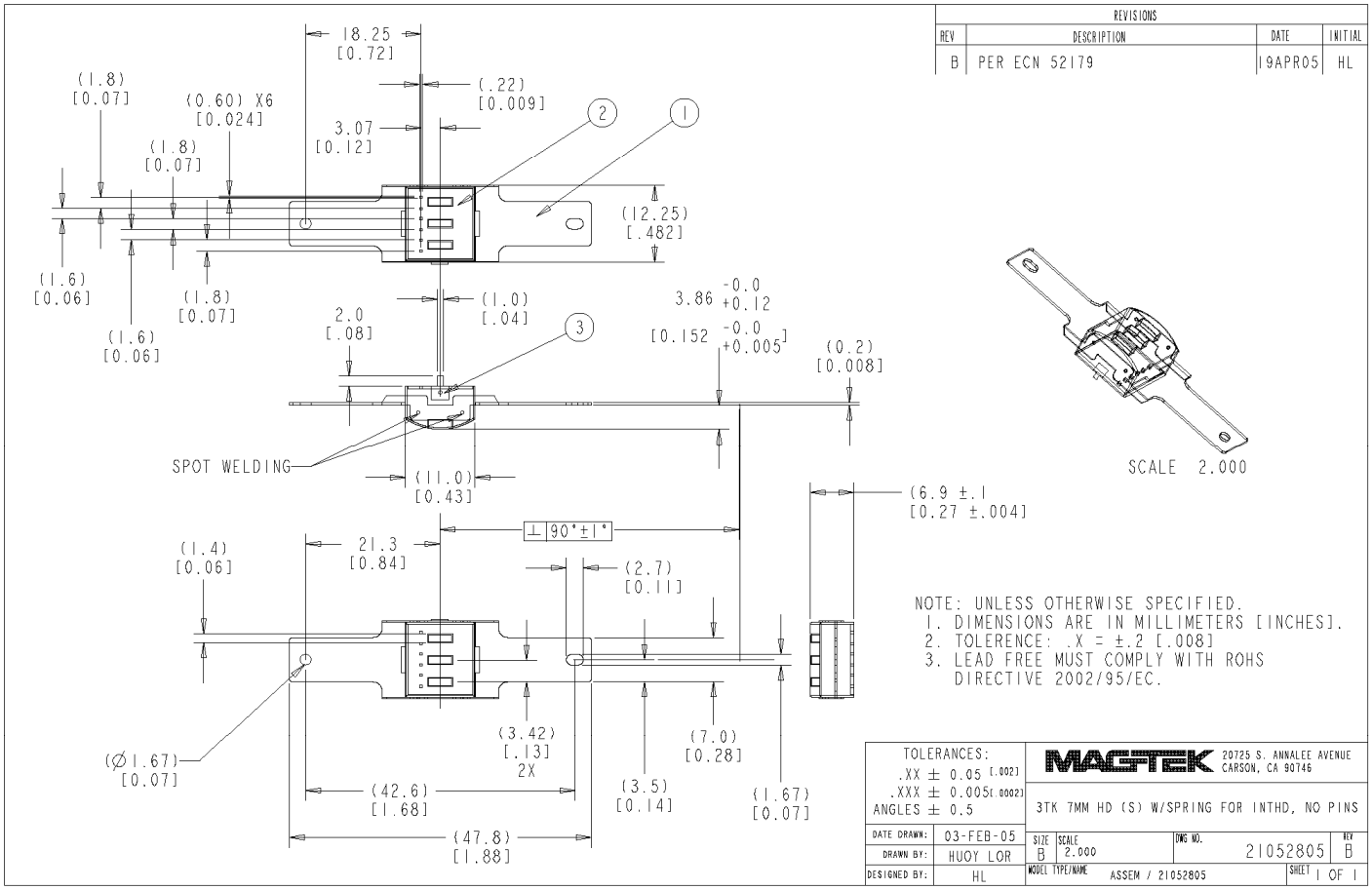


Figure C-12 Dimensions for 90mm Butterfly Spring Model

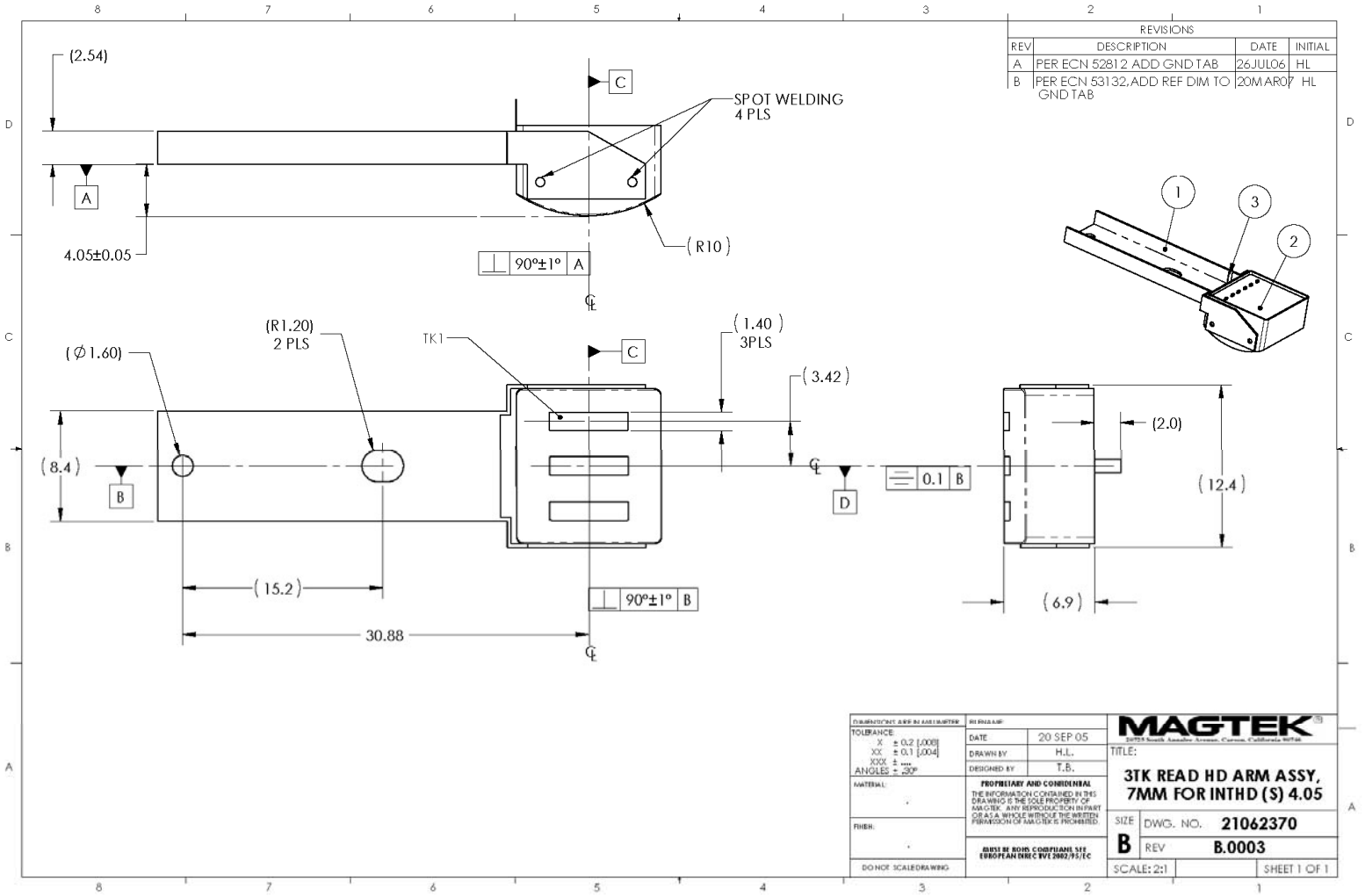


Figure C-13 Dimensions for 4.05mm Beam Arm Model

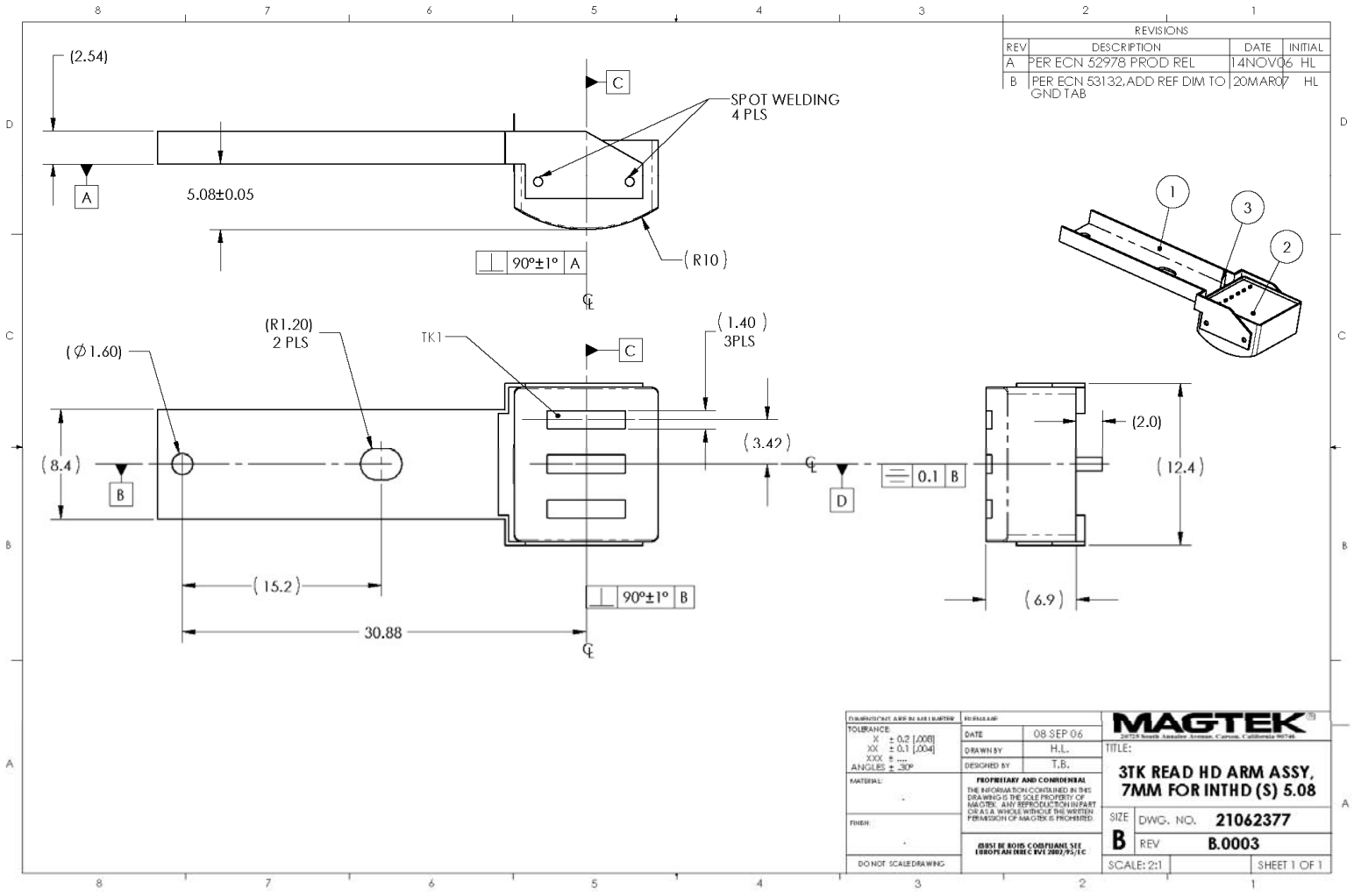


Figure C-14 Dimensions for 5.08mm Beam Arm Model

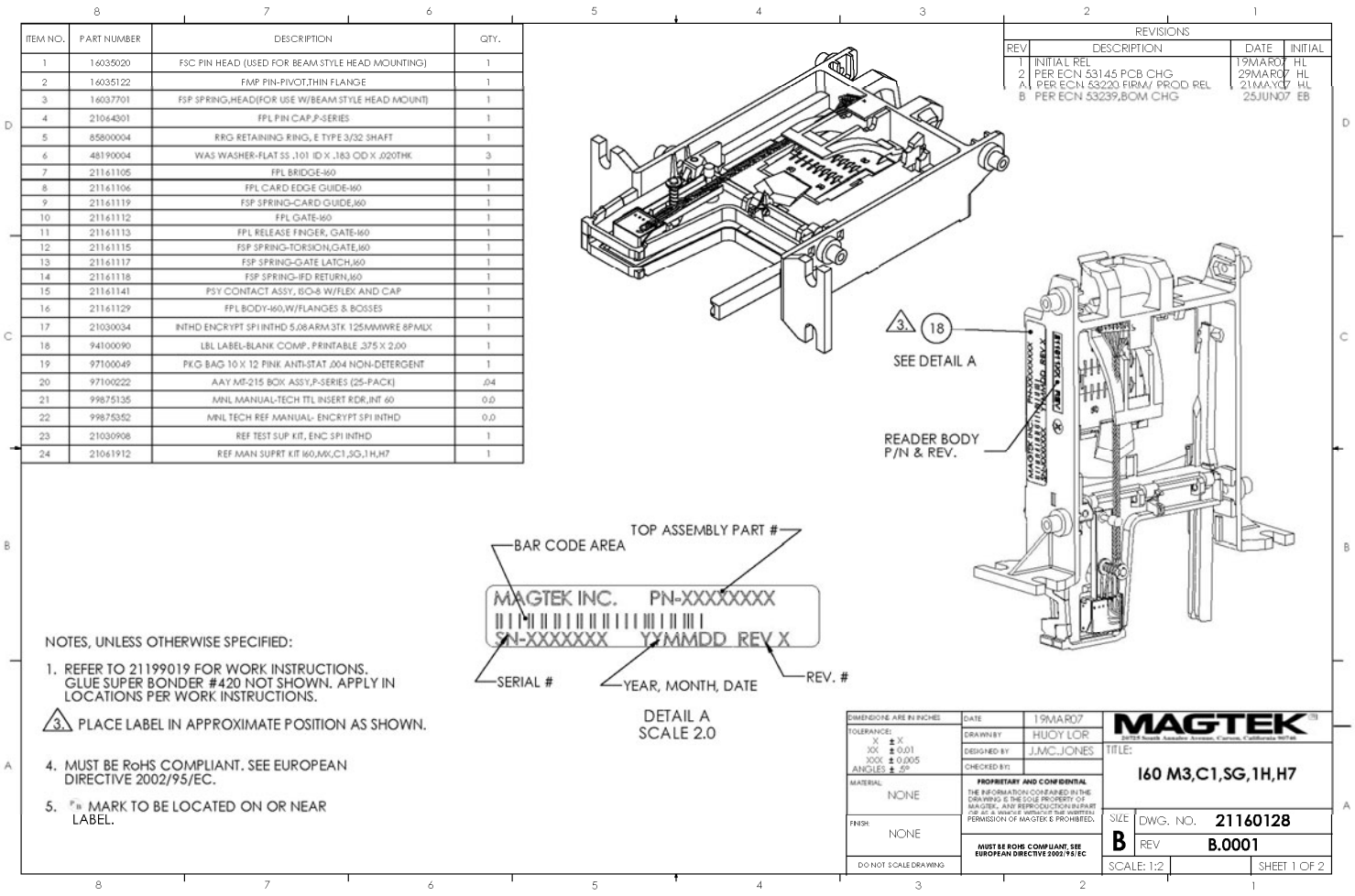
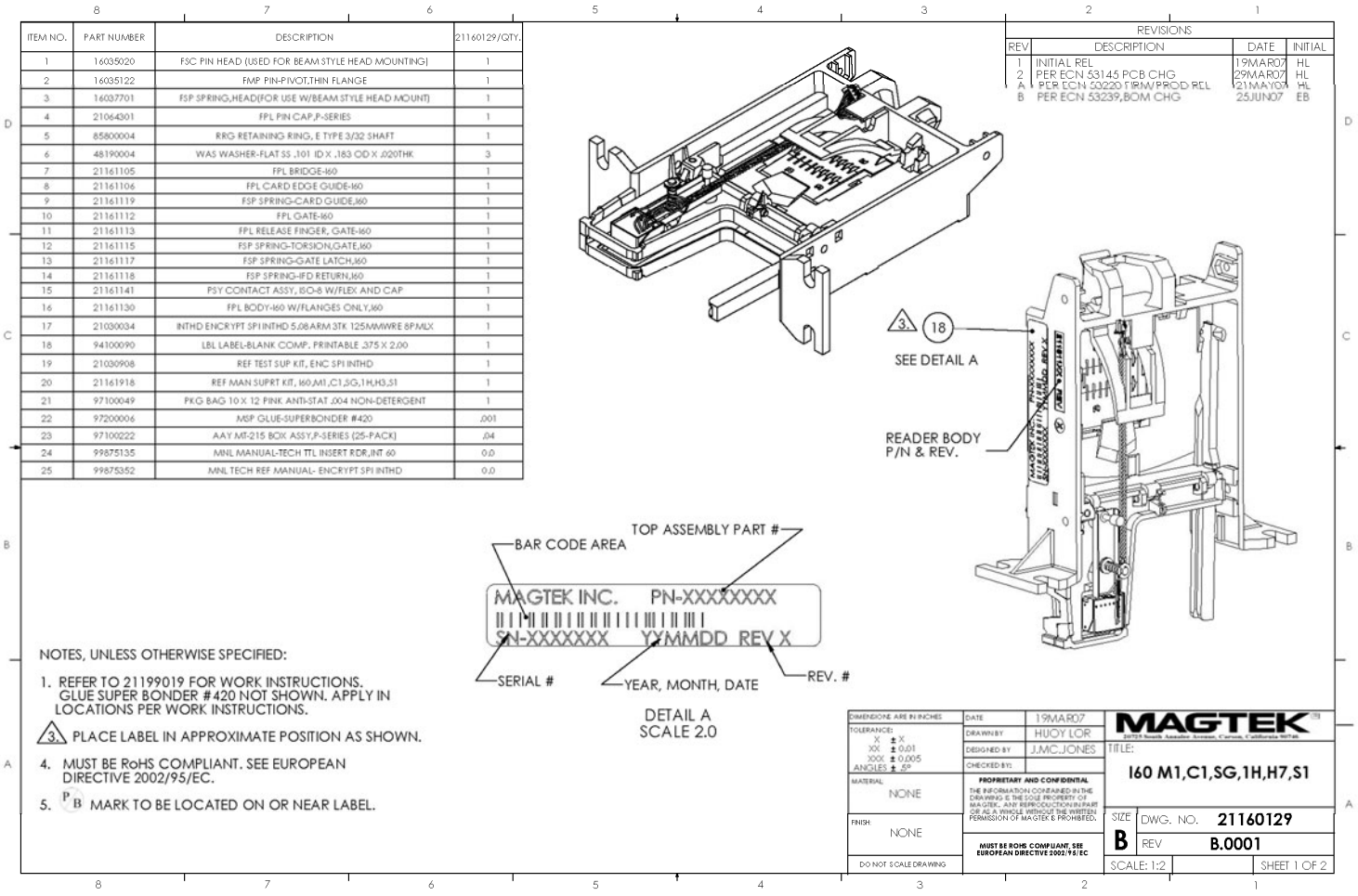


Figure C-15 IntelliStripe 60 Front & Side Bezel



ITEM NO.	PART NUMBER	DESCRIPTION	21160129/QTY.
1	16035020	FSC PIN HEAD (USED FOR BEAM STYLE HEAD MOUNTING)	1
2	16035122	FMP PIN-PIVOT,THIN FLANGE	1
3	16037701	FSP SPRING,HEAD(FOR USE W/BEAM STYLE HEAD MOUNT)	1
4	21064301	FPL PIN CAP,P-SERIES	1
5	85800004	RRG RETAINING RING, E TYPE 3/32 SHAFT	1
6	48190004	WAS WASHER-FLAT SS ,101 ID X ,183 OD X .020THK	3
7	21161105	FPL BRIDGE-I60	1
8	21161106	FPL CARD EDGE GUIDE-I60	1
9	21161119	FSP SPRING-CARD GUIDE,I60	1
10	21161112	FPL GATE-I60	1
11	21161113	FPL RELEASE FINGER, GATE-I60	1
12	21161115	FSP SPRING-TORSION,GATE,I60	1
13	21161117	FSP SPRING-GATE LATCH,I60	1
14	21161118	FSP SPRING-IFD RETURN,I60	1
15	21161141	FSY CONTACT ASSY, ISO-8 W/FLEX AND CAP	1
16	21161130	FPL BODY-I60 W/FLANGES ONLY,I60	1
17	21030034	INTHD ENCRYPT SPI INTHD 5.08 ARM 3TK 125MMWRE 8P.MLX	1
18	94100090	LBL LABEL-BLANK COMP. PRINTABLE .375 X 2.00	1
19	21030908	REF TEST SUP KIT, ENC SPI INTHD	1
20	21161918	REF MAN SUPRT KIT, I60,M1,C1,SG,1H,H3,S1	1
21	97100049	PKG BAG 10 X 12 PINK ANTI-STAT .004 NON-DETERGENT	1
22	97200006	MSP GLUE-SUPERBONDER #420	.001
23	97100222	AAY MT-215 BOX ASSY,P-SERIES (25-PACK)	.04
24	99875135	MNL MANUAL-TECH TTL INSERT RDR,INT 60	0.0
25	99875352	MNL TECH REF MANUAL- ENCRYPT SPI INTHD	0.0

REVISIONS			
REV	DESCRIPTION	DATE	INITIAL
1	INITIAL REL	19MAR07	HL
2	PER ECN 53145 PCB CHG	29MAR07	HL
A	PER ECN 50220 FIRM/PROD REL	21MAY07	HL
B	PER ECN 53239,BOM CHG	25JUN07	EB

NOTES, UNLESS OTHERWISE SPECIFIED:

1. REFER TO 21199019 FOR WORK INSTRUCTIONS. GLUE SUPER BONDER #420 NOT SHOWN. APPLY IN LOCATIONS PER WORK INSTRUCTIONS.
3. PLACE LABEL IN APPROXIMATE POSITION AS SHOWN.
4. MUST BE RoHS COMPLIANT. SEE EUROPEAN DIRECTIVE 2002/95/EC.
5. (P) (B) MARK TO BE LOCATED ON OR NEAR LABEL.

DIMENSIONS ARE IN INCHES	DATE	19MAR07	MAGTEK
TOLERANCES: X ± X, XX ± 0.01, XXX ± 0.005, ANGLES ± .5°	DRAWN BY	HUOY LOR	
	DESIGNED BY	J.MC.JONES	TITLE: I60 M1,C1,SG,1H,H7,S1
	CHECKED BY:		
MATERIAL: NONE	PROPRIETARY AND CONFIDENTIAL		
FINISH: NONE	MUST BE ROHS COMPLIANT, SEE EUROPEAN DIRECTIVE 2002/95/EC		SIZE B, DWG. NO. 21160129, REV B.0001
DO NOT SCALE DRAWING			SCALE: 1:2, SHEET 1 OF 2

Figure C-16 IntelliStripe 60 Front Bezel

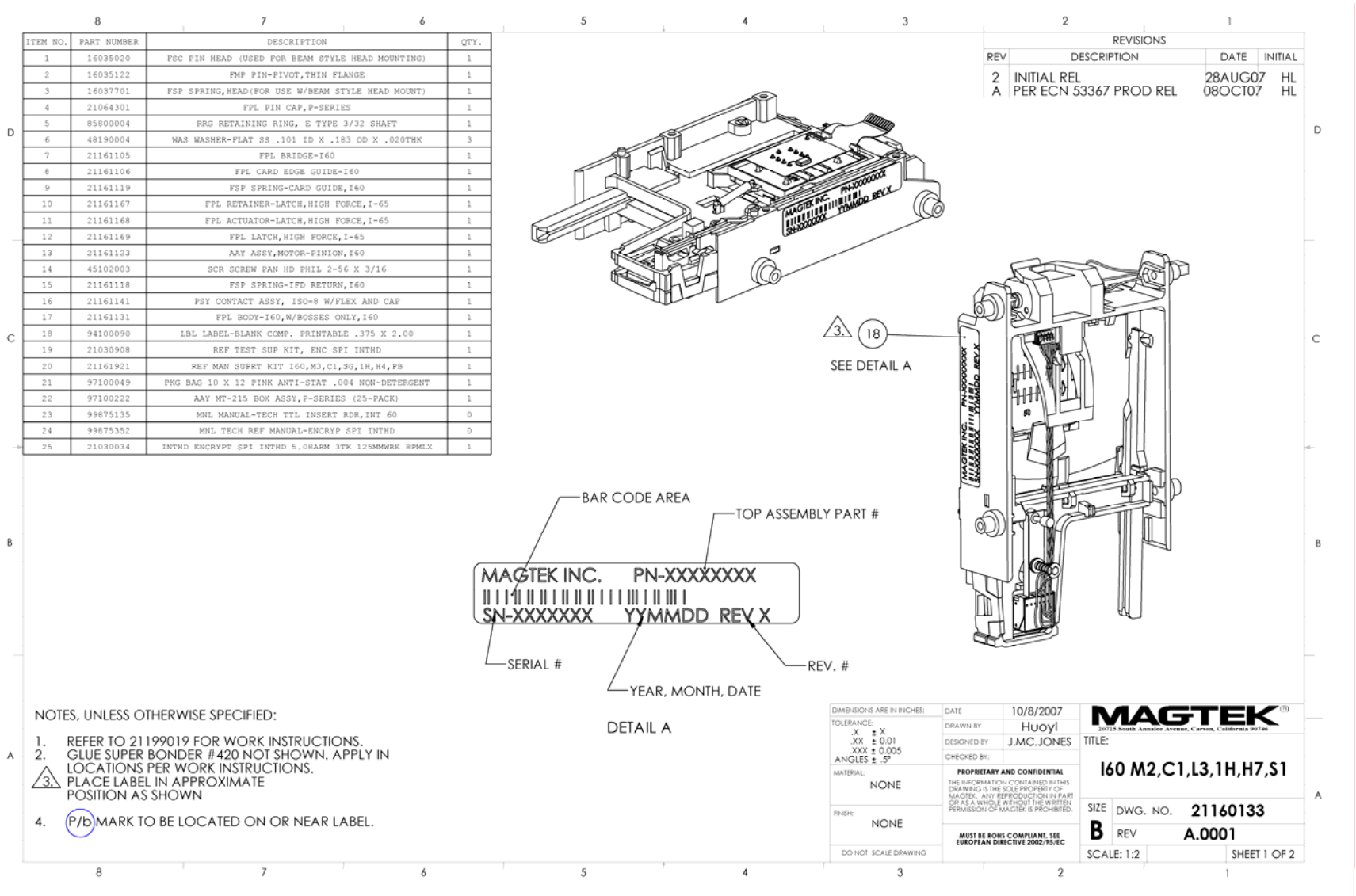
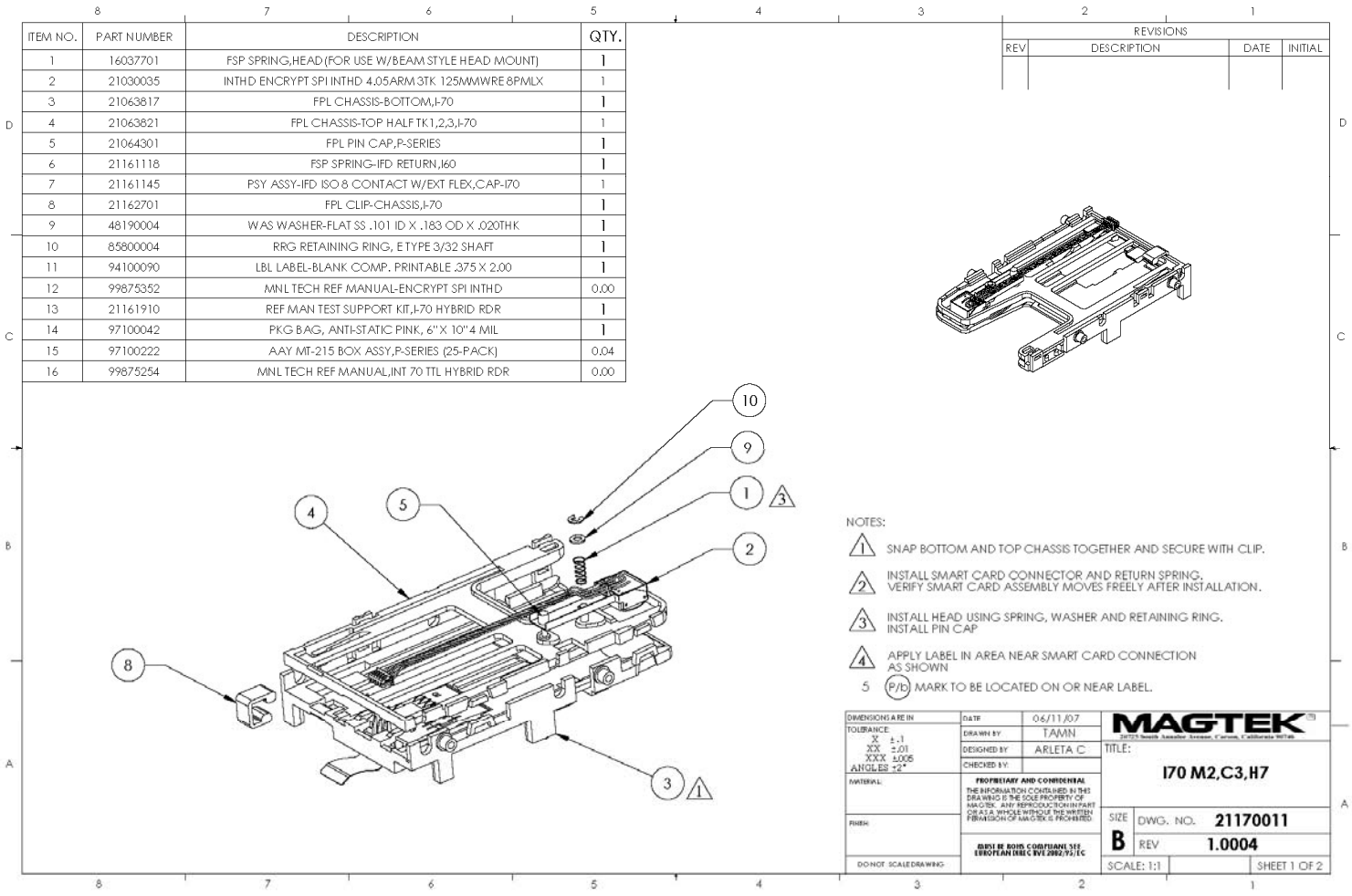


Figure C-17 IntelliStripe 60 Side Bezel with Latch



ITEM NO.	PART NUMBER	DESCRIPTION	QTY.
1	16037701	FSP SPRING,HEAD (FOR USE W/BEAM STYLE HEAD MOUNT)	1
2	21030035	INTHD ENCRYPT SPI INTHD 4.05ARM 3TK 125MMWRE 8PMLX	1
3	21063817	FPL CHASSIS-BOTTOM,I-70	1
4	21063821	FPL CHASSIS-TOP HALF TK1,2,3,I-70	1
5	21064301	FPL PIN CAP,P-SERIES	1
6	21161118	FSP SPRING-IFD RETURN,I60	1
7	21161145	PSY ASSY-IFD ISO 8 CONTACT W/EXT FLEX,CAP-I70	1
8	21162701	FPL CLIP-CHASSIS,I-70	1
9	48190004	WAS WASHER-FLAT SS .101 ID X .183 OD X .020THK	1
10	85800004	RRG RETAINING RING, E TYPE 3/32 SHAFT	1
11	94100090	LBL LABEL-BLANK COMP. PRINTABLE .375 X 2.00	1
12	99875352	MNL TECH REF MANUAL-ENCRYPT SPI INTHD	0.00
13	21161910	REF MAN TEST SUPPORT KIT,I-70 HYBRID RDR	1
14	97100042	PKG BAG, ANTI-STATIC PINK, 6" X 10" 4 MIL	1
15	97100222	AAY MT-215 BOX ASSY,P-SERIES (25-PACK)	0.04
16	99875254	MNL TECH REF MANUAL,INT 70 TTL HYBRID RDR	0.00

REVISIONS			
REV	DESCRIPTION	DATE	INITIAL

NOTES:

1. SNAP BOTTOM AND TOP CHASSIS TOGETHER AND SECURE WITH CLIP.
2. INSTALL SMART CARD CONNECTOR AND RETURN SPRING. VERIFY SMART CARD ASSEMBLY MOVES FREELY AFTER INSTALLATION.
3. INSTALL HEAD USING SPRING, WASHER AND RETAINING RING. INSTALL PIN CAP
4. APPLY LABEL IN AREA NEAR SMART CARD CONNECTION AS SHOWN
5. P/b MARK TO BE LOCATED ON OR NEAR LABEL.

DIMENSIONS ARE IN	DATE	06/11/07	MAGTEK
TOLERANCE X ±.1, XX ±.01, XXX ±.005, ANGLES ±2°	DRAWN BY	TAMN	TITLE: I70 M2,C3,H7
	DESIGNED BY	ARLETA C	
	CHECKED BY		
MATERIAL	PROPRIETARY AND CONFIDENTIAL THE INFORMATION CONTAINED IN THIS DRAWING IS THE SOLE PROPERTY OF MAGTEK. ANY REPRODUCTION IN PART OR AS A WHOLE WITHOUT THE WRITTEN PERMISSION OF MAGTEK IS PROHIBITED.		SIZE B, DWG. NO. 21170011, REV 1.0004
FINISH			
DO NOT SCALE DRAWING	MUST BE ROHS COMPLIANT, SEE EUROPEAN DIREC TIVE 2002/95/EC		SCALE: 1:1, SHEET 1 OF 2

Figure C-18 IntelliStripe 70 Side Bezel