TEXAS INSTRUMENTS

Reader Series 4000

S4100 Multi-Function Reader Module RF-MGR-MNMN

Low Frequency Library Reference Guide

11-01-21-701 October 2003

First Edition - October 2003

This is the first edition of this manual. It describes the **TI Series 4000 Reader.**

It contains a description of the following reader module:

S4100 Multi-Function Reader Module P/N: **RF-MGR-MNMN-N0**

Texas Instruments (TI) reserves the right to make changes to its products or services or to discontinue any product or service at any time without notice. TI provides customer assistance in various technical areas, but does not have full access to data concerning the use and applications of customer's products

Therefore, TI assumes no liability and is not responsible for customer applications or product or software design or performance relating to systems or applications incorporating TI products. In addition, TI assumes no liability and is not responsible for infringement of patents and/or any other intellectual or industrial property rights of third parties, which may result from assistance provided by TI.

TI products are not designed, intended, authorized or warranted to be suitable for life support applications or any other life critical applications which could involve potential risk of death, personal injury or severe property or environmental damage.

Read This First

About This Manual

This reference guide for the Series 4000 Multi-Function (13.56 MHz & 134.2 KHz) Reader is designed for use by TI customers who are engineers experienced with RFID Systems and Radio Frequency Identification Devices (RFID).

Device Name	Boot Loader Firmware Version
RF-MGR-MNMN-N0	1.02

The Regulatory, safety and warranty notices that must be followed are provided in Chapter 2.

Conventions

The following pictograms and designations are used in the operating instructions:

WARNING:

A WARNING IS USED WHERE CARE MUST BE TAKEN, OR A CERTAIN PROCEDURE MUST BE FOLLOWED, IN ORDER TO PREVENT INJURY OR HARM TO YOUR HEALTH.

CAUTION:

This indicates information on conditions, which must be met, or a procedure, which must be followed, which if not needed could cause permanent damage to the system.

Note:

Indicates conditions, which must be met, or procedures which must be followed, to ensure proper functioning.

Information:

Indicates conditions or procedures that should be followed to ensure proper functioning of the system.

If You Need Assistance

Application Centers are located in Europe, North and South America, the Far East and Australia to provide direct engineering support.

For more information, please contact your nearest TIRIS Sales and Application Center. The contact addresses can be found on our home page: http://www.tirfid.com.

Numerical Representations

Unless otherwise noted, numbers are represented as decimal.

Hexadecimal numbers are represented with the suffix $_{16}$, e.g. $A5F1_{16}$

Binary numbers are represented with the suffix $_2$, e.g. 1011_2

Byte representations: the least significant bit (lsb) is bit 0 and the most significant bit (msb) is bit 7.

Document Overview

Chapter 1

Introduction

Topic **Page**

1.1 Overview

The following sections define and detail the Protocol functionality in the LF Module of the MFR Base Application. This information includes LF Protocol Commands and the data/parameters associated with them.

The MFR reader uses the Texas Instruments TMS3705A LF ASIC chip to modulate the signal from the reader to the token and to read the information transmitted back from the token to the reader. The TXCT pin of the LF ASIC is used to control the information sent to the token and the SCIO pin of the LF ASIC is used to read data from the token. These lines must be controllable down to the microsecond level for reliable results. The information is sent to the LF ASIC at 9600 baud and is returned from the LF ASIC at 15.6 K baud.

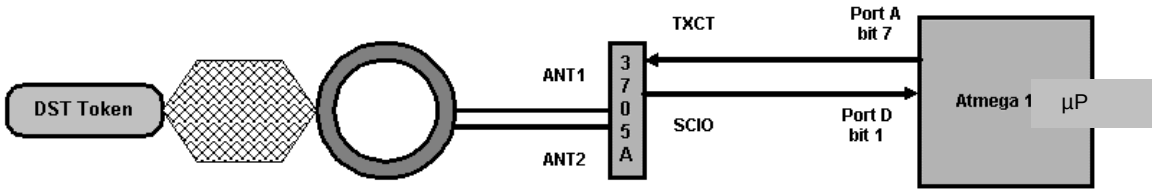

Figure 1-1: MFR Functional Overview

When executed, a Power Burst is sent to charge the LF token within the RF field. While some functions may require a modulated signal to transmit the data bits for the required command, programming and encryption require a second Power Burst to boost the power during these operations. Each Power Burst will be in the range of milliseconds in duration and typically the first burst will be 50 milliseconds. The TXCT line is toggled low for the Power Burst duration then raised high when finished. The data is sent LSB first for each byte of data, with each bit of data OFF for a period of time and then ON for a period of time. The communications to the LF ASIC is 9600 baud, with each bit requiring 1 millisecond of time for most LF Read instructions and 2 milliseconds for most Write instructions. The default MFR read times are:

High Bit – OFF 120 microseconds and ON 880 microseconds
Low Bit – OFF 480 microseconds and ON 520 microseconds

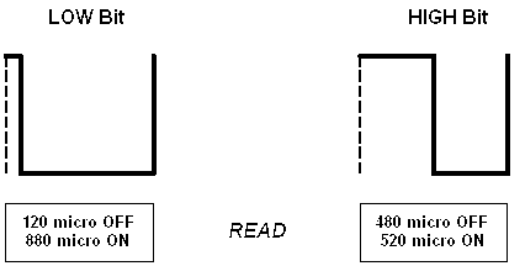

Figure 1-2: MFR Default Read Times

The default Write timings are:

High Bit – OFF 300 microseconds and ON 1700 microseconds
Low Bit – OFF 1000 microseconds and ON 1000 microseconds

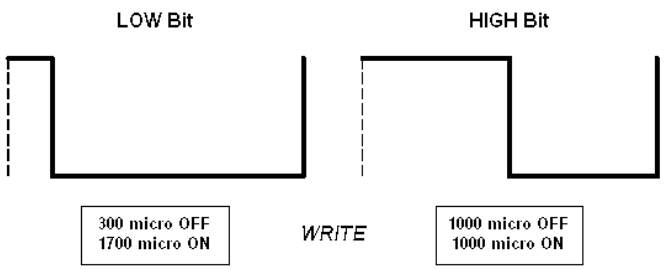

Figure 1-3: MFR Default Write Times

Each Pass Through command allows the programmer control of each of these durations.

When using the General Challenge DST command the reader sends the Write Address, followed by 5 bytes of random data. A Selective Challenge includes a Password Byte between the Write Address and the random data. A second power burst is sent after the modulated data is finished to give extra power for the encryption process.

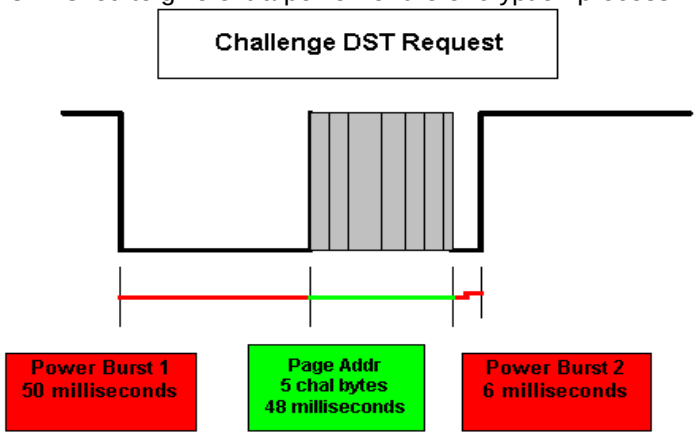

Figure 1-4: MFR General DST Challenge Timing

During the DST Challenge cycle the LF ASIC receives the data from the LF token, converts it and transmits it out the SCIO pin at 15.6 K baud. Each byte has one Start Bit that is high and one Stop Bit that is low. There are 8 data bits in between these stop and start bits and they are LSB first and inverted. The firmware starts to sample the SCIO line after the data has been transmitted to the DST token. It detects when the SCIO line goes high and then waits half a bit time, to make certain it is a start bit and not noise. There are 9 more samples, one bit time apart, to read the 8 data bits and stop bit. The bit time for 15.6 K baud is 64 microseconds. The sample results are translated from LSB to MSB and inverted to the proper bit values. The data is then passed back to the calling function.

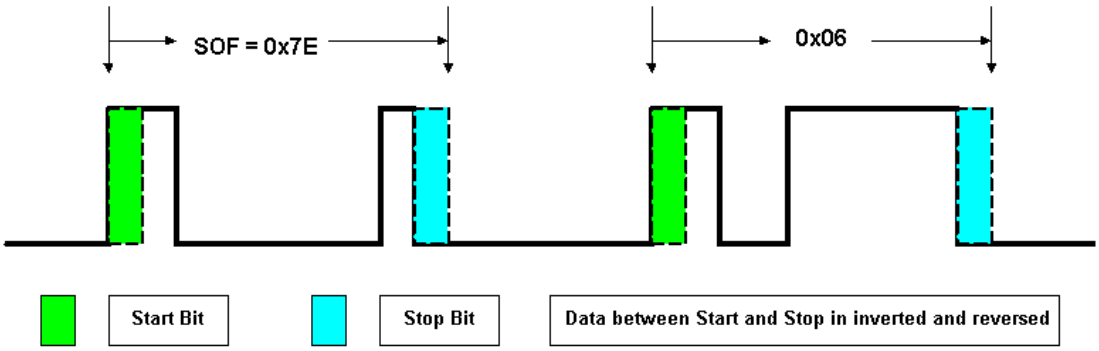

Figure 1-5: MFR General DST Data Flow Timing

1.1.1 Find Token Request (41_{16})

The host application can send the MFR reader a Request Packet to check if a token is present. This packet contains a loop count parameter that sets the maximum number of times the MFR reader searches for each RF format in the Priority Table. This parameter allows the host to have control of how many times the terminal samples for each RF format before determining that no token is present. The function exits and returns a response packet when it gets the first valid read.

This function provides the host with a great deal of flexibility. It is possible to search for a variety of transponders or a single type of token. If multiple RF formats have been selected, the function returns the first valid token that is read. The terminal doesn't complete the maximum number of loops specified unless it fails to detect a valid token. The terminal doesn't return every type of token that may be in the field - just the first one read. Note that the priority table determines the order in which the terminal looks for the RF format when the <*Cmd1*> field is set to the Application Layer $\mathbf{01}_{16}$. The terminal ignores the Priority Table when the <*Cmd1*> field points directly to a specific RF Entity ID. This document provides examples of how the Find Token Request will access the LF Entity Module, when the <*Cmd1*> field is set to both the Application Layer $\mathbf{01}_{16}$ and the LF Entity Layer $\mathbf{06}_{16}$.

The MFR reader responds with **ERROR_NONE** in the *Response Status Byte* field when an LF token has been successfully read. The next byte in the <*Data Layer*> of the Response Packet reflects the type of token that was read. This byte is set to $\mathbf{06}_{16}$ when the token is a DST, R/O, or R/W LF format. The RF poll stops once a valid token is found or the maximum number of loops have occurred. If a valid token is not found within the loop count selected, the MFR terminal responds with an **ERROR_TOKEN_NOT_PRESENT** for the *Response Status Byte*.

The <*Cmd1*> field determines if the MFR reader uses the Token Priority Table to select the RF formats or directs the reader to search only for a specific RF format. The terminal only uses the RF Priority Table when the <*Cmd1*> field is pointing to the Application Layer $\mathbf{01}_{16}$. The MFR reader defaults to search for transponders in the default order when the RF Priority Table is empty. The LF format is the 5th format checked when the reader is set to the default priority. The MFR reader ignores LF transponders when the LF format has not been selected in the Priority Table and the <*Cmd1*> field is pointing to the Application Layer.

It is possible to bypass the Priority Table by setting the <*Cmd1*> field to a value other than the Application Layer. Currently the MFR reader can select from 1 to 5 RF formats to check during the each loop through the Priority Table.

The Find Token Request changes from an Application Layer Command to an Entity Module Command when the <*Cmd1*> field is set to a specific library value, rather than the Application Layer.

The typical Request Packet contains a Maximum Loop Count that sets the maximum number of times the MFR Module searches for the token. This function gives a great deal of flexibility. It is possible to search for a variety of transponders or a single type of token. If multiple token formats are selected, the function returns the first token that is read. The reader doesn't wait the entire time duration specified, unless it fails to detect a token. The reader doesn't return every type of token present - just the first one read. A Loop count of $\mathbf{00}_{16}$ instructs the reader to stay in an endless loop waiting for a token.

The Find Token Request supports Digital Signature Transponders (*DST*), Read Only Transponders (*RO*) or Read Write Transponders (*RW*). The successful LF Response Packet <*Data Layer*> contains a Response Status Byte $\mathbf{00}_{16}$, the LF Entity ID $\mathbf{06}_{16}$ and then the LF token data. The data is as follows:

DST – 1-byte Manufacturing ID, 3-byte Serial Number
RO – 1-byte <SOF> ($7E_{16}$), 8-byte Identifier
RW – 1-byte <SOF> (FE_{16}), 8-byte Identifier

The Response Packet for a valid LF read for a Find Token Request returns the same information when the <*Cmd1*> field is directed to the LF Module Library or to the Application Layer. The only difference is that the <*Cmd1*> field of the Response Packet reflects where the Request Packet had directed the request.

Application Layer Find Token Request

Direct the <*Cmd1*> field to the Application Layer of a MFR reader with the Default Priority Table set. Set the Loop count to $\mathbf{0A}_{16}$ so the reader loops through the Priority table a maximum of 10 times. The Default Priority table checks for 14443-A, 14443-B, 15693, Tag-it™, and LF transponders. The reader checks each RF format for every loop through the table. This function exits and returns the token data when a valid read has been detected. Transponders can be brought into the field as long as this is done before the terminal has completed the maximum number of loops. Examples are provided for the LF module's ability to detect DST, RO and RW transponders with the Find Token Request.

Request packet: (**01 09 00 03 01 41 0A 41 BE**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	09 00	Packet Length 9 bytes
Device ID	03	Terminal is MFR
Command 1	01	Application Layer
Command 2	41	Find Token Request
Timeout	0A	10 loops maximum
BCC	41 BE	LRC and ~LRC

Response packet: (**01 0E 00 03 01 41 00 06 06 FA 04 00 B2 4D**)
Response when a valid **DST** token has been detected.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0E 00	Packet Length 14 bytes
Device ID	03	Terminal is MFR
Command 1	01	Application Layer
Command 2	41	Find Token Request
Status Byte	00	ERROR_NONE
Entity ID	06	LF DST Library
MID	06	Merchant ID
Serial #	FA 04 00	Tag # 1274
BCC	B2 4D	LRC and ~LRC

Response Packet: (**01 13 00 03 01 41 00 06 7E 7C F3 EF 01 00 00 00 00 48 B7**)
Note that the Response is 19 bytes – The <*SOF*> and the 8-byte **R0** Identifier are returned.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19bytes
Device ID	03	Terminal is MFR
Command 1	01	Application Layer
Command 2	41	Find Token Request
Status Byte	00	ERROR_NONE
Entity ID	06	LF DST Library
SOF	7E	R0 *SOF* character

Identifier	7C F3 EF 01 00 00 00 00	RO Identifier
BCC	48 B7	LRC and ~LRC

Response Packet: (**01 13 00 03 01 41 00 06 FE 18 17 16 15 14 13 12 11 A1 5E**)
Note that the Response is 19 bytes – The <*SOF*> and the 8-byte **RW** Identifier are returned.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	01	Application Layer
Command 2	41	Find Token Request
Status Byte	00	ERROR_NONE
Entity ID	06	LF DST Library
SOF	FE	RW SOF character
Identifier	18 17 16 15 14 13 12 11	RW Identifier
BCC	A1 5E	LRC and ~LRC

Note that it is also possible that there is no LF token in the field during the duration of the loop counts. Also, there may be multiple valid LF transponders in the field that will cause an invalid read. It is also possible to have a single valid LF token in the field while executing the Find Token Request but the LF format is not in the Priority Table. All of these cases will result in an error message that resembles the following Response Packet.

Response Packet: (**01 09 00 03 01 41 01 4A B5**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	09 00	Packet Length 9 bytes
Device ID	03	Terminal is MFR
Command 1	01	Application Layer
Command 2	41	Find Token Request
Status Byte	01	ERROR_TOKEN_NOT_PRESENT
BCC	4A B5	LRC and ~LRC

LF Module Find Token Request

The Find Token Request can be directed specifically to the LF Module Library when the <*Cmd1*> filed is set to the LF Entity ID $\mathbf{06}_{16}$. This creates a situation where the Find Token Request only looks for LF transponders, regardless of the current Priority Table in the MFR reader. The LF Format does not even have to be in the Priority Table for this function. The results are the same as they were for the Application Layer Find Token Request, except this returns the LF token data when LF is not in the Priority table, and the <*Cmd1*> value in the Response Packet will reflect that it was directed to the LF library. Examples are provided for the same DST, RO, and RW transponders that where used in the Application Layer Find Token Request to demonstrate that the only difference is the <*Cmd1*> field and resulting BCC values.

Request Packet: (**01 09 00 03 06 41 0A 46 B9**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	09 00	Packet Length 9 bytes
Device ID	03	Terminal is MFR
Command 1	06	Library Layer – LF Module
Command 2	41	Find Token Request

Timeout	0A	10 loops maximum
BCC	46 B9	LRC and ~LRC

Response packet: (**01 0E 00 03 06 41 00 06 06 FA 04 00 B5 4A**)
Response when a valid **DST** token has been detected.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0E 00	Packet Length 14 bytes
Device ID	03	Terminal is MFR
Command 1	06	Library Layer – LF Module
Command 2	41	Find Token Request
Status Byte	00	ERROR_NONE
Entity ID	06	LF DST Library
MID	06	Merchant ID
Serial #	FA 04 00	Tag # 1274
BCC	B5 4A	LRC and ~LRC

Response Packet: (**01 13 00 03 06 41 00 06 7E 7C F3 EF 01 00 00 00 00 4F B0**)
Note that the Response is 19 bytes – The <*SOF*> and the 8-byte **R0** Identifier are returned.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	Library Layer – LF Module
Command 2	41	Find Token Request
Status Byte	00	ERROR_NONE
Entity ID	06	LF DST Library
SOF	7E	R0 SOF character
Identifier	7C F3 EF 01 00 00 00 00	RO Identifier
BCC	4F B0	LRC and ~LRC

Response Packet: (**01 13 00 03 06 41 00 06 FE 18 17 16 15 14 13 12 11 A6 59**)
Note that the Response is 19 bytes – The <*SOF*> and the 8-byte RW Identifier are returned.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	Library Layer – LF Module
Command 2	41	Find Token Request
Status Byte	00	ERROR_NONE
Entity ID	06	LF DST Library
SOF	FE	RW SOF character
Identifier	18 17 16 15 14 13 12 11	RW Identifier
BCC	A6 59	LRC and ~LRC

1.1.2 Pass-Through Request (45_{16})

The MFR reader will call the LF Module Pass Through function when <*Cmd1*> field is set to **06_{16}** and the *Command 2* field is set to **45_{16}** in the Request Packet. The <*Data Layer*> is stripped from the Request Packet and passed to the LF Module Library to allow the Host full control over the LF ASIC. This allows the MFR reader to function in a similar manner to the TI Micro-Reader.

The <*Data Layer*> portion must be passed in the following format:

[PB1][PB2][T_OFF_H][T_ON_H][T_OFF_L][T_ON_L][DATA]

The first two parameters are bytes and represent Power Burst durations in milliseconds. The following 4 parameters are integer values for the ON and OFF times in milliseconds. The DATA portion is the modulated data sent between power bursts, while the Write Address is the first byte of modulated data for DST transponders but not RO or RW transponders. The following sections detail how this information is used to perform specific LF functionality.

Information:

The LF Pass Through command can be used to communicate with Digital Signature Transponder (DST), Read Only (RO), and Read Write (RW) transponders. Some commands issued for DST devices may work with RO or RW transponders. The response packet's content reflects the type of token that responded. This function provides a way to isolate and test the LF Module functions without having to make any modifications to the Application Layer.

The Pass Through function can be used to reproduce any of the other LF functionality. This function does not parse and validate the response data from the token. The data is returned for the host to parse and validate. This function forces the user to send the Power Burst durations and ON and OFF timings each time. Most of the LF functions hard code the values such as Power Burst ON and OFF durations and the Write Address, while the Pass Through requires this information each time.

The following sections provide some examples of how the LF Pass Through command can be used to replicate the functionality of some of the LF functions. Note that the values used in these examples are the same as the hard coded Power burst and ON OFF timing values for the functions that are being replicated. The response packets can be compared to those from the real functions to show the difference. It is also possible to tweak the power burst and timing values should someone desire to achieve different results from that received from the hard coded function.

LF Pass Through – Read DST Request

The Read DST Request can be issued to a DST token by sending a 50 millisecond Power Burst and then the 8-bit Write Address to indicate the DST page to read. The initial power Burst is sufficient to energize the token and NO second Power Burst is required.

Information:

While this command is designed for a DST token, it will also generate a response from a Read Only or Read Write as well. Note that a **RW** or **RO** response length is two bytes longer than the **DST** response

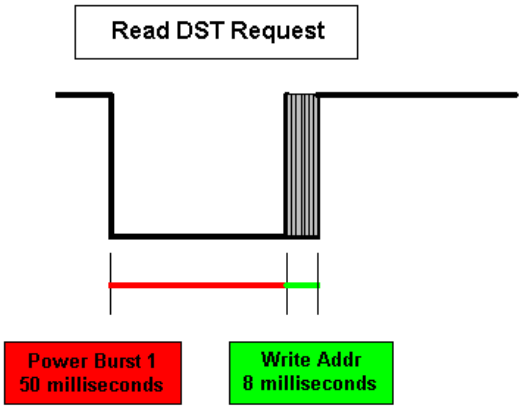

Figure 1-6: Read DST Request

The following diagram illustrates the ON and OFF times for the modulated data for a standard LF Read DST Request.

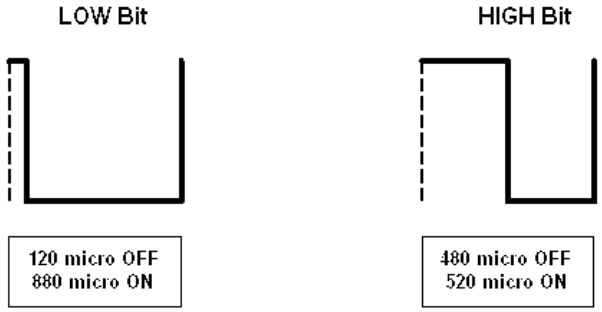

Figure 1-7: Read DST Request Timing

The READ DST Request is actually a Write DST Command that requests to read the DST Page 3 data. Please note that the DST token returns the contents of Page 1, Page 2 and Page 3 when there is a request to read any of those pages. The difference is the Read Address, which indicates the Page selected and the status of that particular page. The Read Address for Page 3 is **$0C_{16}$** for a token with Page 3 unlocked and **$0E_{16}$** for a token with Page 3 locked. With a valid LF DST token in the RF field, send a valid Read DST Request via the Pass-Through Request to the MFR reader and validate the data received.

Request Packet: (**01 13 00 03 06 45 32 00 78 00 70 03 E0 01 08 02 0C 8C 73**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Pass Through Request
Power Burst 1	32	ON 50 milliseconds
Power Burst 2	00	No second Power Burst
T OFF High	78 00	120 microseconds
T ON High	70 03	880 microseconds
T OFF Low	E0 01	480 microseconds
T ON Low	08 02	520 microseconds
Write Address	0C	Page 3
BCC	8C 73	LRC and ~LRC

Response Packet: (**01 13 00 03 06 45 00 7E 06 10 06 FA 04 00 0E 7F 77 C4 3B**)

This is the response for a DST token with Serial # 1274 and Page 3 Locked. All of the data from the token is returned and it is up to the host to validate the data.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Set Driver Request
Status Byte	00	ERROR_NONE
SOF	7E	DST Start of Frame
Password Byte	06	Password – 06
Identifier Byte	10	Identifier – 10
Manufacturing ID	06	Manufacturer Code
Serial #	FA 04 00	Token # 1274
Read Address	0E	Page 3 – Locked
Token CRC 16	7F 77	CRC 16 on DST packet
BCC	C4 3B	LRC and ~LRC

RO and RW transponders can be energized by and will respond to the Read DST request. The 50-millisecond Power Burst is all that is required and the Write Address value will be ignored. Both the RO and RW transponders return the <*SOF*> character, the 64-bit Identifier, the 16-bit CRC on the Identifier and the EOF character. The RO token uses $\mathbf{7E}_{16}$ as the <*SOF*> and EOF character while the RW transponders use $\mathbf{FE}_{16}$. Example Response Packets for both the RO and RW transponders are as follows:

Response Packet: (**01 15 00 03 06 45 00 7E 7C F3 EF 01 00 00 00 00 FA 38 7E F7 08**)
This is the response for a RO token.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	15 00	Packet Length 21 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Set Driver Request
Status Byte	00	ERROR_NONE
SOF	7E	RO Start of Frame
Identifier	7E 7C F3 EF 01 00 00 00	Token 64-bit Identifier
Token CRC 16	38 7E	CRC 16 on RO packet
EOF	7E	RO End of Frame
BCC	F7 08	LRC and ~LRC

Response Packet: (**01 15 00 03 06 45 00 FE 12 34 56 78 90 09 87 65 DD 79 FE 83 7C**)
This is the response for a RW token.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	15 00	Packet Length 21 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Set Driver Request
Status Byte	00	ERROR_NONE
SOF	FE	RW Start of Frame
Identifier	12 34 56 78 90 09 87 65	Token 64-bit Identifier
Token CRC 16	DD 79	CRC 16 on RO packet
EOF	FE	RW End of Frame
BCC	83 7C	LRC and ~LRC

LF Pass-Through – Challenge DST Request

The Challenge DST Request can be issued to a DST token by sending a 50 millisecond Power Burst and then the 8-bit Write Address to indicate the DST Page 4, then the 40-bit Random Number. The initial power Burst is NOT sufficient to energize the token during the encryption process, and a second 6-millisecond 2nd Power Burst is required.

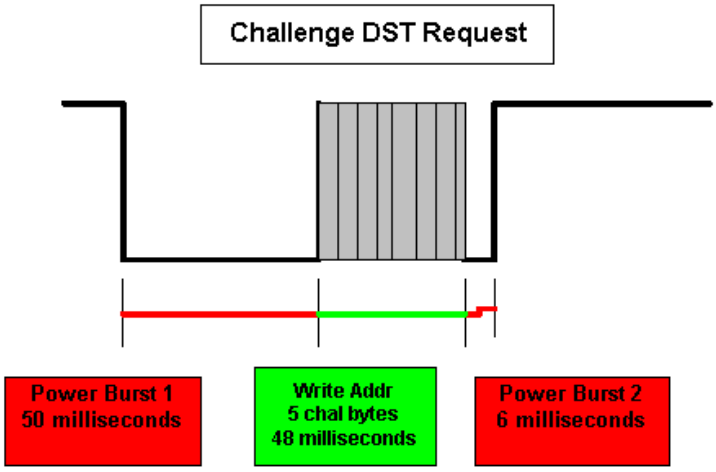

Figure 1-8: Challenge DST Request Timing

The following diagram illustrates the ON and OFF times for the modulated data for a standard LF Challenge DST Request.

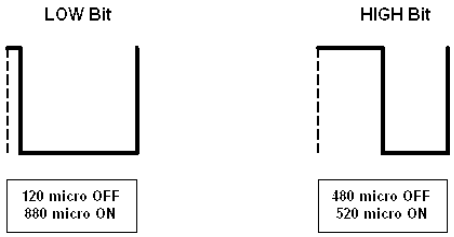

Figure 1-9: Challenge DST Request Timing

The READ DST Request is actually a Write Command that requests to read the DST Page 3 data.

Note that the DST token returns the contents of Page 1, Page 2 and Page 3 when there is a request to read any of those pages. The difference is the Read Address. The Read Address reflects the Page selected and the status of that particular page. The Read Address for Page 3 is **0C**$_{16}$ for a token with Page 3 unlocked and **0E**$_{16}$ for a token with Page 3 locked. Place a valid LF DST token in the RF field, then send a valid Read DST Request via the Pass-Through Request to the MFR reader and validate the data received.

Send a valid Challenge DST Request via the Pass-Through Request to the MFR device with the COM port set to 9600 8N1 and validate the data received. Have a valid LF DST token in the field.

Request Packet: (**01 18 00 03 06 45 32 06 78 00 70 03 E0 01 08 02 10 11 88 66 CC 55 FB 04**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	18 00	Packet Length 24 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Pass Through Request
Power Burst 1	32	ON 50 milliseconds
Power Burst 2	06	ON 6 milliseconds
T OFF High	78 00	120 microseconds
T ON High	70 03	880 microseconds
T OFF Low	E0 01	480 microseconds
T ON Low	08 02	520 microseconds
Write Address	10	Page 4
5 Random Bytes	11 88 66 CC 55	5 bytes of Random Data
BCC	FB 04	LRC and ~LRC

Response Packet: (**01 13 00 03 06 45 00 7E FA 04 00 95 6E DF 12 04 63 83 7C**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Set Driver Request
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Serial #	FA 04 00	Token # 1274
Digital Signature	95 6E DF	3 MSB of DST Computation result
Read Address	12	Page 4 - Page is Locked
Token CRC 16	04 63	CRC 16 on DST packet
BCC	83 7C	LRC and ~LRC

Note that the Pulse Burst causes a RO or RW token to respond just as illustrated in the Pass-Through Read DST example. Those transponders simply look for a 50-millisecond Power Burst before they send back the Read information.

LF Pass-Through – Write to RW Token Request

The Write RW Token Request can be issued to a Read Write (WR) token by sending a 50 millisecond Power Burst and then 122 bits of modulated data. A second 15-millisecond Power Burst is required to keep the RW token charged. Note that the Write timings are about twice as long as the Read timings. The 122 bits of modulated data is comprised of the following elements:

Key Word – Forced to **BB**$_{16}$
Password – Forced to **EB**$_{16}$
Write Data – 64-bits of data to write to token
CRC bytes – 16-bits CRC on data
Write Frame – Forced to **0300**$_{16}$

Information:

The Pulse Width durations are longer when Programming the token than the durations used to Read a token.

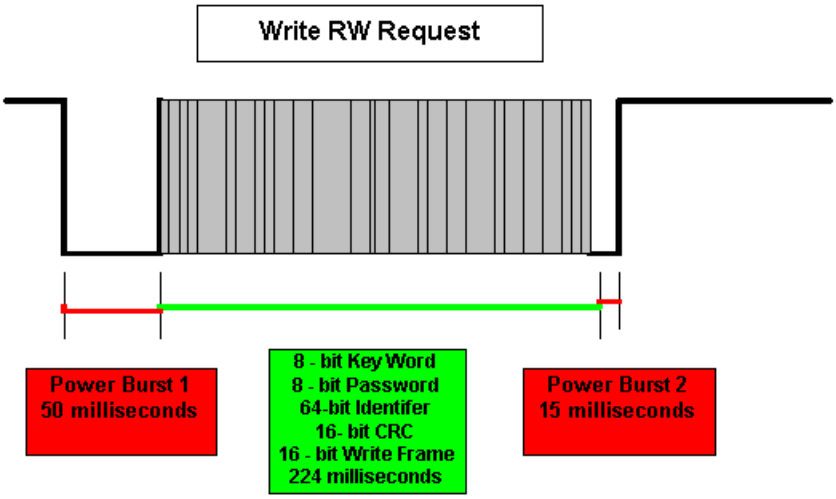

Figure 1-10: Write to RW Token Request Timing

The following diagram illustrates the ON and OFF times for the modulated data for a standard LF Write RW Request.

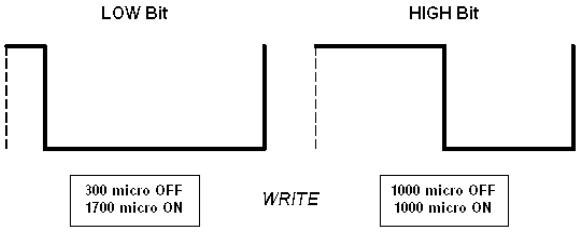

Figure 1-11: Write to RW Token Request Timing

Request Packet: (**01 20 00 03 06 45 32 0F 2C 01 A4 06 E8 03 E8 03 BB EB 18 17 16 15 14 13 12 11 DE B0 00 03 E6 19)**

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	20 00	Packet Length 32 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Pass Through Request
Power Burst 1	32	ON 50 milliseconds
Power Burst 2	0F	ON 15 milliseconds
T OFF High	2C 01	300 microseconds
T ON High	A4 06	1700 microseconds
T OFF Low	E8 03	1000 microseconds
T ON Low	E8 03	1000 microseconds
Page Address	BB	Key Word
Password	EB	Password
RW tag Identifier	18 17 16 15 14 13 12 11	64-Bit Identifier
CRC 16	DE B0	CRC on Identifier
Write Frame	00 03	RW Write Frame
BCC	E6 19	LRC and ~LRC

Response Packet: (**01 15 00 03 06 45 00 FE 18 17 16 15 14 13 12 11 DE B0 FE 32 CD**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	15 00	Packet Length 21 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	45	Pass Through
Status Byte	00	ERROR_NONE
SOF	FE	RW Start of Frame
64-bit Identifier	18 17 16 15 14 13 12 11	Identifier field
CRC 16	DE B0	CRC 16 on Identifier data
EOF	FE	RW End of Frame
BCC	32 CD	LRC and ~LRC

LF Pass-Through – Write DST Token Request

The Write DST Request is able to perform most of the DST functionality. For example the Read DST and Challenge DST examples provided above are actually executing examples of Write DST functions. Do not confuse the term Write with Program. The Write DST functions indicate that the function sent (or wrote) modulated data to the DST token. This data may be a request to Read data from the Token, or to Program the token.

There are too many possibilities to cover all of the potential Write DST Request packets. These will be covered in greater detail in the WRITE DST section of this document. It is important to note though that it is possible to recreate them all with the LF Pass-Through function.

The first Power Burst is typically 50-milliseconds. The Second Power Burst is not required unless Programming the token or encrypting data. The first byte of modulated data is always the Write Address. The ON/OFF timings for the High and Low bits are similar to those used in the Pass Through – Read DST example when reading data from the token, and similar to the Write RW example when Programming the DST token.

General Write functions do not require the 16-bit CRC computation to be transmitted to the DST token, but Selective Write functions will require the 16-bit CRC computation to be sent. This is true for the General Encrypt and Selective encrypt functions as well.

There are several stipulations to follow when using the Write DST functions. It is not recommended that a user utilize these functions unless they have a good understanding of DST transponders and they are attempting to optimize a particular command. A Write DST function has been provided that will provide for most of the overhead, like setting the Pulse Burst durations and calculating the CRC value and transmitting it when required. This function only requires the proper Write Address and then the additional data.

1.1.3 Read RO-RW (61_{16})

The Read RO-RW function is able to read and return the data from Read Only (RO) and Read Write (RW) transponders. Firstly it is important to distinguish between the two LF token types. The most obvious difference is that the RO transponders use a <*SOF*> and <*EOF*> character **7E**$_{16}$ and the RW transponders use the character **FE**$_{16}$. Some additional information is provided for both token formats.
The Read Only transponders are programmed and locked at manufacturing time. The only functionality supported for the RO transponders is to read the contents stored within them. A 50-millisecond power burst enables the RO token to recognize the request and respond with the data stored in its memory. An RO token returns a total of 12 data bytes.

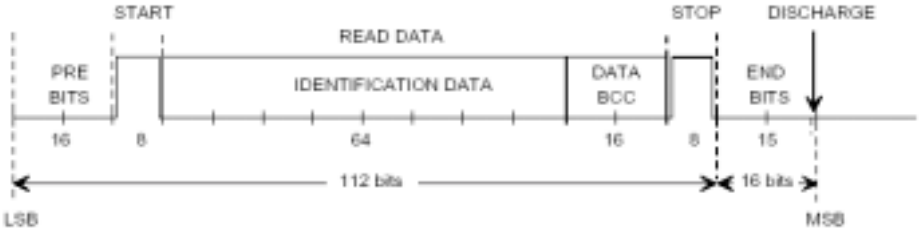

Figure 1-12: Read RO Data Structure

There is a Start of Frame <*SOF*> character at the beginning of the data and an End of Frame <*EOF*> character at the end of the token data. Both the <*SOF*> and <*EOF*> characters are **7E**$_{16}$ for RO transponders. A 64-bit Identifier follows the <*SOF*> character. The Identifier bytes are transmitted least significant byte first. A CRC 16 value is calculated on the Identifier data and is stored in the token after the identifier data. The CRC 16 calculation starts with an Init value of 0x0000 and uses the polynomial of 0x1021. The last character is the <*EOF*> character.

The Read Write transponders may or may not be programmed at manufacturing time. A blank token will have a default Identifier of 5555555555555555. The functionality supported for the RW transponders is to read the contents stored within them and also to write the 64-bit identifier within the token. A 50-millisecond power burst allows the RW token to recognize the request and it responds with the data stored in its memory.

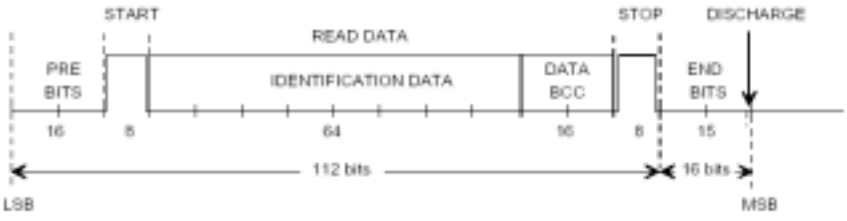

Figure 1-13: Read RW Data Structure

There is a Start of Frame <*SOF*> character at the beginning of the data and an End of Frame <*EOF*> character at the end of the token data. Both the <*SOF*> and <*EOF*>

characters will be **FE**$_{16}$ for RW transponders. The 64-bit Identifier is sent in the 8 bytes following the SOF character. The Identifier bytes is transmitted the least significant byte first. A CRC 16 value is calculated on the identifier data and it is stored in the token after the identifier data. The CRC 16 calculation starts with an Init value of 0x0000 and uses the polynomial of 0x1021. The last character in the token is the <*EOF*> character.

This function sends a power burst for 50 milliseconds and then waits for a response from the RO or RW token. The signal on the LF ASIC SCIO pin is translated into data bytes. The <*SOF*> character is validated and the CRC 16 is calculated and compared to that read from the token. The response byte is set to **ERROR_NONE** and the <*SOF*>, the 64-bit identifier, 16-bit CRC, and EOF are returned in the response packet. The response byte errors are:

ERROR_INVALID_CRC – CRC did not match
ERROR_INVALID_START_BYTE - No **7E**$_{16}$ / **FE**$_{16}$ Start Byte read
ERROR_NO_DATA_READ - No data received on SCIO pin
ERROR_DATA_TRUNCATED - Destination buffer too small for all data read

Note that the same results may be achieved with the Pass-Through command. The Page address is not passed and this function validates the <*SOF*> and CRC, while the Pass-Through command does not. This function also sets the ON and OFF times for both the HIGH and LOW bits.
Note: RO and RW transponders have both an SOF and an EOF with a 64-bit Identifier value and a 16-bit CRC. It is possible to identify the type of token read though, because the RO transponders use **7E**$_{16}$ for the <*SOF*> and <*EOF*> while RW transponders use **FE**$_{16}$.

Request Packet: (**01 08 00 03 06 61 6D 92**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	08 00	Packet Length 8 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	61	Read RO / RW Request
BCC	6D 92	LRC and ~LRC

Response Packet: (**01 15 00 03 06 61 00 7E 7C F3 EF 01 00 00 00 00 FA 38 7E D3 2C**)
This is an example of a response when a **RO** token has been read.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	15 00	Packet Length 21 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	61	Read RO / RW
Status Byte	00	ERROR_NONE
SOF	7E	RO Start of Frame
RO Tag data	7C F3 EF 01 00 00 00 00	8 data bytes LSB first
Token CRC 16	FA 38	CRC 16 on DST packet
RO EOF	7E	RO End of Frame
BCC	D3 2C	LRC and ~LRC

Response Packet: (**01 15 00 03 06 61 00 FE 18 17 16 15 14 13 12 11 DE B0 FE 16 E9**) This is the result from a RW token read. Notice that both have a 64-bit identifier field but the <*SOF*> and <*EOF*> characters differ.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	15 00	Packet Length 21 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	61	Read RO / RW
Status Byte	00	ERROR_NONE
SOF	FE	RW Start of Frame
RW Tag data	18 17 16 15 14 13 12 11	8 data bytes LSB first
Token CRC 16	DE B0	CRC 16 on DST packet
RW EOF	FE	RW End of Frame
BCC	16 E9	LRC and ~LRC

1.1.4 Write RW (62_{16})

This function allows the user to program a Read Write (RW) token by stripping out the data in the <*Data Layer*> of the Request Packet and then writing it to the RW token. This function always writes 8 data bytes, (64-bits), of Identifier data to the RW token. This Identifier data is padded with $\mathbf{00}_{16}$ characters when the <*Data Layer*> of the Request Packet has less than 8 bytes of Identifier data. It is only possible to Program 64-bits of Identifier data. This function limits the data to the first 64-bits when the <*Data Layer*> is larger than 8 bytes. This function hard codes all Power Burst durations and sets the ON/OFF timings for the High and Low bits as well as inserting the required values for the Key Word, Password, and Write Frame values. The Identifier information is stripped out of the <*Data Layer*> and transmitted along with the 16-bit CRC value calculated from the Identifier data.

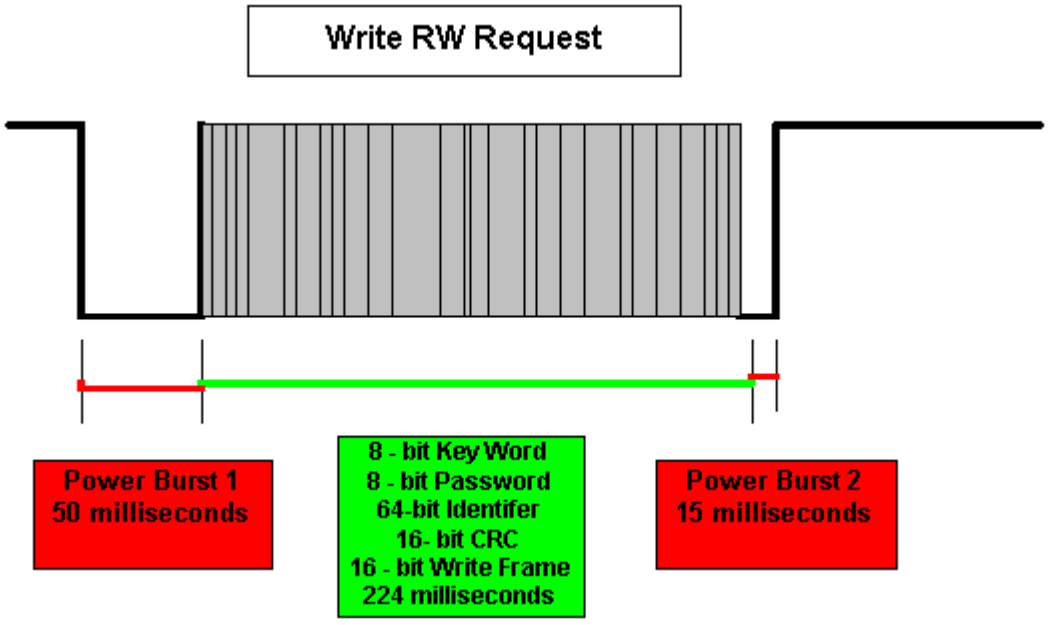

Figure 1-14: Write RW Request Timing

Notice that in Figure 3-16 there are fields required for Write Password, Write Frame and Write Keyword. Those values are hard coded into this function and are not passed by the

Request Packet. The <*Data Layer*> only needs to provide the Data to write to the token. The Hard coded values are:

Write Keyword: BB_{16}
Write Password: EB_{16}
Write Frame : $0x0300_{16}$

In the following example, the 64-bit Identifier value (**11 22 33 44 55 66 77 88)** $_{16}$ is written into a RW token. Note that this function does not require the <*Data Layer*> of the Request Packet to have any information other than the Identifier value to write to the token. The High Low bit timings and Power bursts and other overhead-modulated data are calculated and inserted automatically by this function. The Pass Through function would require all of that information in the <*Data Layer*>.

Request Packet: (**01 10 00 03 06 62 11 22 33 44 55 66 77 88 FE 01**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	10 00	Packet Length 16 bytes
Device ID	03	Terminal is MFR
Command 1	06	Write RW Layer
Command 2	62	Read RO / RW Request
RW Tag Data	11 22 33 44 55 66 77 88	64-bits of data to program
BCC	FE 01	LRC and ~LRC

Response Packet: (**01 11 00 03 06 62 00 11 22 33 44 55 66 77 88 FF 00**)
Notice the response just returns the new 64-bit Identifier value. This shows the write worked.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	11 00	Packet Length 17 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	62	Write RW
Status Byte	00	ERROR_NONE
RO Tag data	11 22 33 44 55 66 77 88	8 data bytes LSB first
BCC	FF 00	LRC and ~LRC

1.1.5 Read DST (63_{16})

The Read DST function, reads and return the data from pages 1, 2 and 3 of DST transponders. Because of the in-built security required for the Challenge/ Response, you are never able to read the secret key information stored in page 4

Request Packet: (**01 08 00 03 06 63 6F 90**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	08 00	Packet Length 8 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	63	Read DST Request
BCC	6F 90	LRC and ~LRC

Response Packet: (**01 13 00 03 06 63 00 7E FF 00 06 97 03 00 0E C9 7D DD 22**)
This is an example of a response when a **DST** token has been read.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	63	Read DST
Status Byte	00	ERROR_NONE
SOF	7E	DST Start of Frame
Password byte	FF	Password - FF
Identifier byte	00	Identifier - 00
Man ID	06	Customer code
S/N (LSB first)	97 03 00	Token # 919
Page Address	0E	Page 3
Token CRC 16	C9 7D	CRC 16 on DST packet
BCC	DD 22	LRC and ~LRC

1.1.6 Challenge DST (64_{16})

The Challenge DST function allows the host to add extra security to DST transponder operation. DST transponders can have a five-byte Encryption Key stored on Page 4. This Key information cannot be read from the DST token. A Challenge DST can be issued to the token and the response can be verified to ensure that the token is valid.

The Challenge DST is actually a General Encryption performed with the 5 data bytes stored on Page 4 of the token. The five bytes of Page 4 data are used as the Encryption Key value when performing a DST Calculation. Five Random bytes of data are passed in the <*Data Layer*> of the Request Packet and this value is treated as the data portion for the DST Calculation. This DST Calculation is similar to a single DES and will generate a five-byte result. The three MSB bytes of this result are passed back in the Response Packet as the Digital Signature for the token.

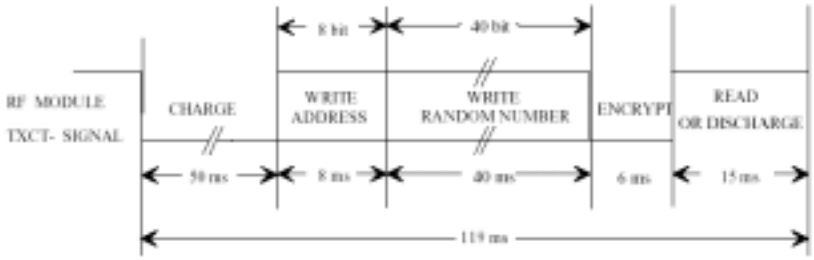

Figure 1-15: Challenge DST Data Structure

The Write Address Page bits select Page 4 and the Status bits are OFF for a General Encrypt.
The General Encrypt always sets the Write Address set to $\mathbf{10}_{16}$. Note that the Write Address and Write Random number are not protected by a CRC value, so there is a small chance that the data could be corrupted during a tag read. This is more likely to happen when the token is at the edge of the read range. When the Digital Signature does not match the expected value, the command should be re-issued.

There is also a Selective Encryption mode that allows the user to select only transponders with the same password as the selected Password (Page 1) value. Transponders with a Password value other than that specified in the Request Packet will be ignored. The Write Address is set to $\mathbf{13}_{16}$ for Selective Encrypt Mode. The Password byte follows the Write Address and precedes the Random number in the <*Data Layer*> of the Request packet.

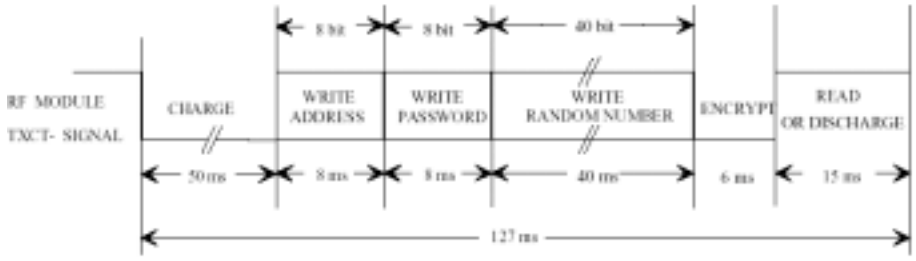

Figure 1-16: Challenge DST Data Structure

The Challenge DST Request Packet includes a five-byte Random Number in *the <Data Layer>* regardless of whether a Generic or Selective Encryption Mode is being issued. This Random number is run through a DST Calculation along with the five-byte Encryption Key read from Page 4 on the DST token. This is similar to running a DES computation and there will be a five-byte result from the DST calculation of these two five byte values. The first three bytes of the result are returned in the <*Data Layer*> of the Response Packet to represent the Digital Signature.

This function sends a Power Burst for 50 milliseconds then transmits the Write Address; the five Random Number bytes. This is followed by a second Power Burst of 6-milliseconds and then a wait for a response from a DST token. The signal on the LF ASIC SCIO pin is translated into data bytes and the *CRC 16* is calculated and compared to that that was read from the token. The response byte will be set to **ERROR_NONE** and all 10 data bytes will be returned in the response packet.
The possible response byte errors are:

ERROR_INVALID_CRC – CRC did not match
ERROR_INVALID_START_BYTE - No **$7E_{16}$** Start Byte read
ERROR_NO_DATA_READ - No data received on SCIO pin
ERROR_DATA_TRUNCATED - Destination buffer too small for all data read

Note that similar results may be achieved with the Pass-Through command. This function validates the <*SOF*> and *CRC* on the Response Packet while the Pass-Through command does not.
This function also sets the ON and OFF times for the HIGH and LOW bits of the modulated data.

The following example demonstrates a Challenge DST (General Encrypt) with a known Encryption Key value. The Encryption Key stored on Page 4 is (**11 22 33 44 55)** $_{16}$ for this example. The Random Number passed to the token is (**11 22 33 44 55)** $_{16}$.

Request Packet: (**01 0E 00 03 06 64 10 11 22 33 44 55 6F 90**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0E 00	Packet Length 14 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	64	Challenge DST Request
Write Address	10	General Encrypt
Random Number	11 22 33 44 55	5 byte Random Number
BCC	6F 90	LRC and ~LRC

Response Packet: (**01 13 00 03 06 64 00 7E BC 04 00 4B 49 F2 10 92 95 52 AD**)
Validate the data is correct using the known Encryption Key.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	64	Challenge DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Serial #	BC 04 00	Token # 1212
Signature	4B 49 F2	3 bytes from DST calculation
Read Address	10	Page 4 - Unlocked
Token CRC 16	92 95	CRC 16 on DST packet
BCC	52 AD	LRC and ~LRC

Note that the data is entered and returned LSB first. Thus $(\mathbf{11\ 22\ 33\ 44\ 55})_{16}$ is really $(\mathbf{55\ 44\ 33\ 22\ 11})_{16}$ for both the encryption key and the Random Number. Using the Engineering tool it is possible to confirm this calculation as shown below. The first 3 bytes of the result are returned:

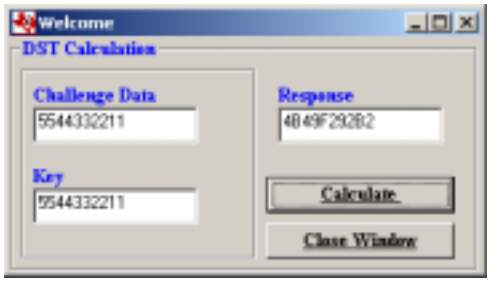

Figure 1-17: DST Response Example

The next example demonstrates a Selective Challenge DST (Selective Encrypt) with the same token as in the previous example. The Password (Page 1) value for that specific token is value $\mathbf{06}_{16}$. This Password value is passed in the <*Data Layer*> of the Request Packet along with the Write Address $\mathbf{13}_{16}$ and Random number $(\mathbf{11\ 22\ 33\ 44\ 55})_{16}$. Note that only Transponders with the Password value of $\mathbf{06}_{16}$ will respond to this request.

Request Packet: (**01 0F 00 03 06 64 13 06 11 22 33 44 55 6B 94**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0F 00	Packet Length 15 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	64	Challenge DST Request
Write Address	13	Selective Encrypt
Password Byte	06	Password - 06
Random Number	11 22 33 44 55	5 byte Random Number
BCC	6B 94	LRC and ~LRC

Response Packet: (**01 13 00 03 06 64 00 7E BC 04 00 4B 49 F2 10 92 95 52 AD**)
Notice that the Response Packet is the same for a General Encrypt and Selective Encrypt.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	64	Challenge DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Serial #	BC 04 00	Token # 1212
Signature	4B 49 F2	3 bytes from DST calculation
Read Address	10	Page 4 - Unlocked
Token CRC 16	92 95	CRC 16 on DST packet
BCC	52 AD	LRC and ~LRC

1.1.7 Write DST (65_{16})

The Write DST function allows the user to have a great deal of control over a DST transponder. The write refers to sending data to the DST transponder, not just writing data into the transponder. It is important to understand a DST transponder before using this command. This brief overview on a DST transponder provides the information required to understand the DST write functionality. The DST transponder is broken into page areas. Each page is reserved for a specific purpose and has a specified number of bits.

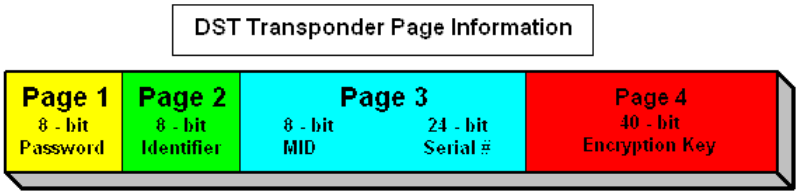

Figure 1-18: DST Page Data

Each packet to the reader for a DST transponder must contain the Write Address. Each valid packet from the DST transponder to the reader will contain the Read Address. Both The Read and Write addresses are a single byte that consists of 6 Page Address Bits followed by 2 Status Bits.

Write Address Status Bits represent the following operations:
- 00 – General Read/ Encrypt mode
- 01 – Program Page
- 10 – Lock Page
- 11 – Selective Read/ Selective Encrypt Mode

Read Address Status Bits represent the following Page or operation status:
- 00 – Read Unlocked Page
- 01 – Program Done
- 10 – Read Locked Page

Page Address Bits for a Read or the Write Address are as follows:
- 000001 – Page 1
- 000010 – Page 2
- 000011 – Page 3
- 000100 – Page 4

A General Read of Page 3 can be used to illustrate how these bits form the Write Address. The Write address has a Page Bit value of **000011**$_2$ and a status value of **00**$_2$. This results in a Write Address of **0C**$_{16}$. The DST response has the Page Bits set to **000011**$_2$ to indicate Page 3 read and Status Bits **10**$_2$ to indicate that Page 3 was Locked or Read Address of **0E**$_{16}$. The DST responds with the Page Bits 000011 and Status Bits 00 or a Read Address of **0C**$_{16}$ when the transponder has Page 3 Unlocked. Note that most DST transponders have page 3 locked when they are programmed by the manufacturer.

The Password Page contents become important when determining the packet the reader sends to the transponder. This function automatically makes the adjustments and sends the proper packet to the transponder. DST transponders default to the value **FF**$_{16}$ in the password field. Note that **FF**$_{16}$ cannot be written into the Password Page, and the Password value **FF**$_{16}$ is never used in password validations. The Host Request Packets must have the password field set to **FF**$_{16}$ when writing to a DST token that has never had the Password Page programmed. This field must match the value in the Password Page when the value was programmed, or the transponder will not reply.

Note that General or Selective Reads can be issued to Pages 1, 2 or 3 and they will return the contents of all three of these pages. The only difference is that the Read Address reflects the Page bits and Status Bits for the Page selected. The status bits are **00**$_{16}$ if the page is unlocked or **01**$_{16}$ when the page has been locked. A Page cannot be unlocked once it is locked and the data on that Page cannot be modified once the Page is locked. Neither a General nor a Selective Read request can be used to read the data stored on Page 4. A General or Selective Encrypt must be used to find if Page 4 is locked or unlocked.

This function has too many options to provide examples of each one. The Write DST Table outlines the supported Write Address values and any additional detail required in the Request Packet.
The response byte is set to **ERROR_NONE** and all data bytes will be returned in the <*Data Layer*> of the Response Packet for a valid read. The Response Status Byte errors are:

ERROR_INVALID_ADDRESS	- Invalid Write Address
ERROR_INVALID_CRC	- CRC did not match
ERROR_INVALID_START_BYTE	- No **7E**$_{16}$ Start Byte read
ERROR_NO_DATA_READ	- No data received on SCIO pin
ERROR_DATA_TRUNCATED	- Destination buffer too small to hold all of the data read

The following sections detail some specific examples about how the Write DST function can be used to perform various DST functions.

General Read Pages 1, 2, 3

The structure of a general Read of Pages 1, 2, and 3 is shown in the following diagram.

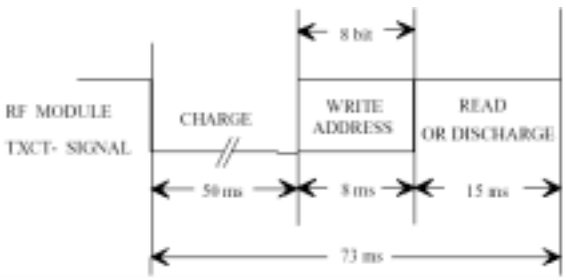

Figure 1-19: General DST Read of Pages 1, 2 & 3

A General Read of any of these pages returns the contents of Pages 1, 2, and 3. The Write Address selects the specific Page being read. Note that the Write Status bits are NOT turned ON when doing a General Read, just the proper Page Bits. The Read Status Bits of the selected Page are returned in the Read Address byte along with the data from Pages 1-3. This shows if that page is Locked or Unlocked. Note these General Reads do not require the Password Byte value. A General Read cannot be performed on Page 4. Read Pages 1, 2, and 3 on a Token that has Pages 1, 2, and 3 Unlocked. Note: it may be hard to find a token with Page 3 Unlocked. To perform a General Read of Page 1 of a DST token.

Request Packet: (**01 09 00 03 06 65 04 6C 93**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	09 00	Packet Length 9 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	04	Select Page 1
BCC	6C 93	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 CC 06 BC 04 00 04 3F F1 B2 4D**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	DST SOF
Password	06	Page 1 – Password - 06
Identifier	CC	Page 2 – Identifier - CC
MID	06	Page 3 – Man. ID - 06
Serial Number	BC 04 00	Page 3 – Serial Number - 1212
Read Address	04	Page 1 Address - Unlocked
DST CRC	3F F1	CRC value of DST data
BCC	B2 4D	LRC and ~LRC

Perform a General Read of Page 2 of the same DST token.
Request Packet: (**01 09 00 03 06 65 08 60 9F**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	09 00	Packet Length 9 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	08	Select Page 2
BCC	60 9F	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 CC 06 BC 04 00 08 53 3B 18 E7**)
Note that the data is the same except for the Read Address and CRC on the data.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Status Byte	00	ERROR_NONE
SOF	7E	DST SOF
Password	06	Page 1 – Password - 06
Identifier	CC	Page 2 – Identifier - CC
MID	06	Page 3 – Man. ID - 06
Serial Number	BC 04 00	Page 3 – Serial Number - 1212
Read Address	08	Page 2 Address - Unlocked
DST CRC	53 3B	CRC value of DST data
BCC	18 E7	LRC and ~LRC

Perform a General Read of Page 3 of the same DST token.
Request Packet: (**01 09 00 03 06 65 0C 64 9B**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	09 00	Packet Length 9 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0C	Select Page 3
BCC	64 9B	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 CC 06 BC 04 00 0C 77 7D 7E 81**)
Note the data is the same except for the Read Address and CRC on data.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Status Byte	00	ERROR_NONE
SOF	7E	DST SOF
Password	06	Page 1 – Password - 06
Identifier	CC	Page 2 – Identifier - CC
MID	06	Page 3 – Man. ID - 06
Serial Number	BC 04 00	Page 3 – Serial Number - 1212
Read Address	0C	Page 3 Address - Unlocked
DST CRC	77 7D	CRC value of DST data
BCC	7E 81	LRC and ~LRC

Selective Read Pages 1, 2, 3

Selective Read of Pages 1, 2, and 3 as shown in the following diagram.

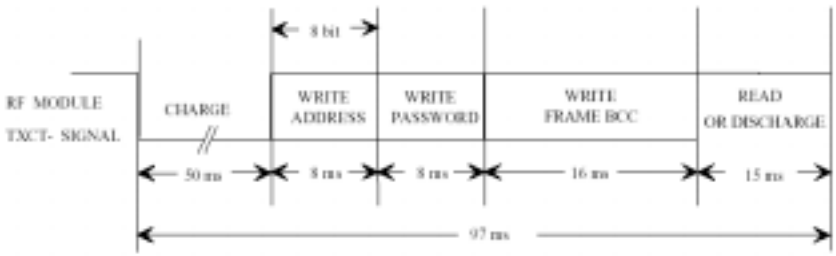

Figure 1-20: Selective DST Read of Pages 1, 2 & 3

The Response Packet has the contents of Pages 1, 2, and 3 in the <*Data Layer*>. The Write Address selects the DST Page read. Notice that the Write Address Byte has the Selective Status Bit turned ON as well as the Page 4 Page Address Bits. The Read Address Byte reflects the proper Page Address Bits and Status Bits for the Page that have been selected in the Write Address. The Response Packet has this Read Address along with the data from Pages 1-3 in the <*Data Layer*>. This indicates if that page is Locked or Unlocked. Notice that the Write Frame BCC characters are required for the Selective Read, while they were not included in the General Read. This is the 16-bit CRC generated on the token data.

The Password Byte is required for any token that has had the Password Byte (Page 1) programmed. The Selective Read will not work when the Password is the default value $\mathbf{FF}_{16}$. The user must pass the value of $\mathbf{FF}_{16}$ when the Password has not been programmed on the token or the reader will treat it as if no token is present. This function calculates the 16-bit CRC and transmits it to the token along with the Write Address and Write Password that have been passed in the <*Data Layer*> of the Request Packet. The Pulse Width and High Low bit ON/OFF timings are set by this function and are not passed as they are in the Pass Through function. Please note that the Response Packet from a Generic Read should return the same information as a Selective Read of the same token, when the same page is read. A Selective Read cannot be performed on Page 4. The following example is a Selective Read of Page 1 for a DST Token where the Password Byte has been programmed $\mathbf{06}_{16}$.

Request Packet: (**01 0A 00 03 06 65 07 06 6A 95**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	07	Selective Read Page 1
Password Byte	06	Password – Page 1 - 06
BCC	6A 95	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 CC 06 BC 04 00 04 3F F1 B2 4D**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	DST SOF
Password	06	Page 1 – Password - 06
Identifier	CC	Page 2 – Identifier - CC
MID	06	Page 3 – Man. ID - 06
Serial Number	BC 04 00	Page 3 – Serial Number - 1212
Read Address	04	Page 1 Address - Unlocked
DST CRC	3F F1	CRC value of DST data
BCC	B2 4D	LRC and ~LRC

This example is a Selective Read of Page 2 for the same DST Token where the Password Byte has been programmed **06_{16}**.

Request Packet: (**01 0A 00 03 06 65 0B 06 66 99**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0B	Selective Read Page 2
Password Byte	06	Password – Page 1 - 06
BCC	66 99	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 CC 06 BC 04 00 08 53 3B 18 E7**)
Note that the information is the same except for the Read Address and the CRC value.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	DST SOF
Password	06	Page 1 – Password - 06
Identifier	CC	Page 2 – Identifier - CC
MID	06	Page 3 – Man. ID - 06
Serial Number	BC 04 00	Page 3 – Serial Number -
Read Address	08	Page 2 Address - Unlocked
DST CRC	53 3B	CRC value of DST data
BCC	18 E7	LRC and ~LRC

This example is a Selective Read of Page 3 for the same DST Token with the Password Byte that has been programmed **06_{16}**.

Request Packet: (**01 0A 00 03 06 65 0F 06 62 9D**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0F	Selective Read Page 3
Password Byte	06	Password – Page 1 - 06
BCC	62 9D	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 CC 06 BC 04 00 0E 65 5E 4D B2**)
Note that the information is the same except for the Read Address and the CRC value.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	DST SOF
Password	06	Page 1 – Password - 06
Identifier	CC	Page 2 – Identifier - CC
MID	06	Page 3 – Man. ID - 06
Serial Number	BC 04 00	Page 3 – Serial Number - 1212
Read Address	0E	Page 3 Address - Locked
DST CRC	65 5E	CRC value of DST data
BCC	4D B2	LRC and ~LRC

Program DST – Page 1 or 2

It is possible to program the data on the Page 1 or Page 2 on the DST transponders as long as the Pages have not been locked. Please note that these pages cannot be programmed once they have been locked. These Pages each contain a single byte of data. Page 1 is the Password Byte and Page 2 is the Identifier Byte. There are two methods of programming Pages 1 or 2. The first method does not transmit the Password value to the token. The second method passes the Password value and will only program DST transponders that match that password.

Program Page 1 or 2 with the Password Page not programmed:

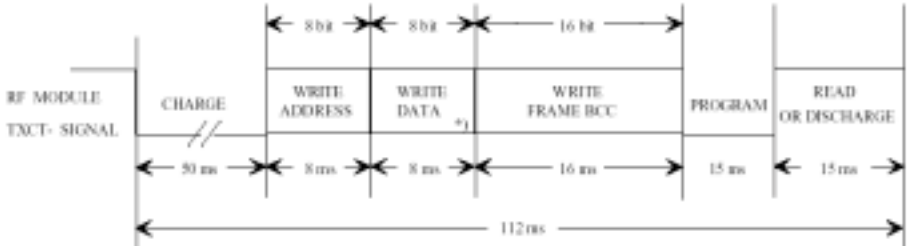

Figure 1-21: Programming Page 1 or 2 with Password Page Not Programmed

Program Pages 1 or 2 with Password Page programmed:

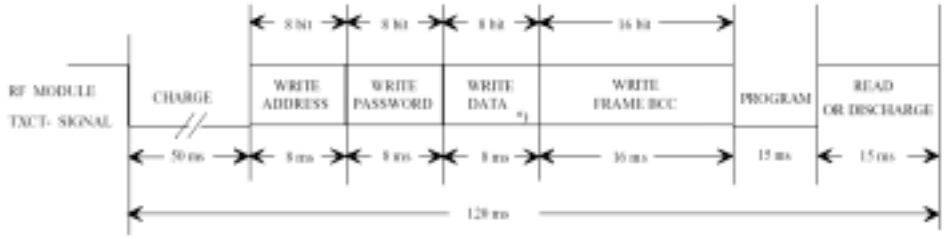

Figure 1-22: Programming Page 1 or 2 with Password Page Programmed

Both methods calculate the CRC 16 value on the data and transmit it to the token. The CRC value is not passed in the Request Packet. Note that the First method is used when the Password value is the default value $\mathbf{FF}_{16}$. The second method is used when the Password is not set to the default value.

Program the Page 2 of a DST token that has had its Password programmed to the value $\mathbf{06}_{16}$. This is similar to the second diagram. The Write Address and Write Data byte are stripped from the <*Data Layer*> of the Request Packet and transmitted to the DST token. The Page Address Bits are $\mathbf{000010}_2$ to indicate Page 2 and the Status Bits are set to $\mathbf{01}_2$ to indicate this page is to be programmed. This results in a Write Address value $\mathbf{09}_{16}$. Page 2 is the Identifier Byte and it will be programmed to $\mathbf{22}_{16}$ in this example.

Request Packet: (**01 0B 00 03 06 65 09 06 22 47 B8**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0B 00	Packet Length 11 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	09	Program Page 2 - Identifier
Password Byte	06	Password – Page 1 - 06
Identifier Value	22	Program Identifier to 22
BCC	47 B8	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 22 06 BC 04 00 09 6B 91 65 9A**)
Validate the Identifier Byte programmed and the Read Address Status Bits.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	06	Page 1 – Password - 06
Identifier Byte	22	Page 2 – Identifier - 22
MID	06	Page 3 – Man. ID - 06
Serial #	BC 04 00	Page 3 – Serial # - 1212
Read Address	09	Page 2 Write Complete
Token CRC 16	6B 91	CRC 16 on DST packet
BCC	65 9A	LRC and ~LRC

It is also possible to change the Password Byte (Page 1) after it has already been programmed. That is, as long as Page 1 has not been locked. For this example the DST Password Byte has been programmed to $\mathbf{06}_{16}$ and Page 1 is Unlocked. Program the Page 1, Password Byte so is changed from $\mathbf{06}_{16}$ to $\mathbf{08}_{16}$. The Page Address Bits are set to 000001 to direct it to the Password byte (Page 1) and Status bits are set to 01 to indicate a Program instruction. The Write Address is set to $\mathbf{05}_{16}$ in the <*Data Layer*> of the Request Packet. This will use the method outlined in the second diagram.

Request Packet: (**01 0B 00 03 06 65 05 06 08 61 9E**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0B 00	Packet Length 11 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	05	Program Page 1 - Password
Password Byte	06	Password – Page 1 - 06
Identifier Value	08	Change Password to 08
BCC	61 9E	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 08 22 06 BC 04 00 05 26 DD 66 99**)
Validate the Password Byte and the Read Address Status Bits.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	08	Page 1 – Password - 08
Identifier Byte	22	Page 2 – Identifier - 22
MID	06	Page 3 – Man. ID - 06
Serial #	BC 04 00	Page 3 – Serial # - 1212
Read Address	05	Page 1 Write Complete
Token CRC 16	26 DD	CRC 16 on DST packet
BCC	66 99	LRC and ~LRC

The first diagram outlines the procedure to program Page 1 or 2 on a DST token that has never had the Password Byte programmed. This example demonstrates how use the Write DST function to Program the Identifier Byte (Page 2) of a DST token that has the default Password $\mathbf{FF}_{16}$. The Write Address will be set to $\mathbf{09}_{16}$ just as it was in the example that programmed Page 2 on a DST token with the Password Byte programmed. The Write Address, Password Byte and new Identifier Byte are in the <*Data Layer*> of the Request Packet. The Password Byte is set to $\mathbf{FF}_{16}$ to represent a token with default Password and the new Identifier Byte for this example is $\mathbf{11}_{16}$.

Request Packet: (**01 0B 00 03 06 65 09 FF 11 8D 72**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0B 00	Packet Length 11 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	09	Program Page 2 - Identifier
Password Byte	FF	Password – Page 1 - Default
Identifier Value	11	Program Identifier to 11
BCC	8D 72	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E FF 11 06 1A 04 00 09 09 65 9F 60**)
Validate the Identifier Byte programmed and the Read Address Status Bits.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	FF	Page 1 – Password - Default
Identifier Byte	11	Page 2 – Identifier - 11
MID	06	Page 3 – Man. ID - 06
Serial #	1A 04 00	Page 3 – Serial # - 1050
Read Address	09	Page 2 Write Complete
Token CRC 16	09 65	CRC 16 on DST packet
BCC	9F 60	LRC and ~LRC

The first diagram outlines the procedure to program Page 1 or 2 on a DST token that has never had the Password Byte programmed. This example demonstrates how to use the Write DST function to Program the Password Byte (Page 1) on a DST token that has the default Password $\mathbf{FF}_{16}$. The Write Address is set to $\mathbf{05}_{16}$ just as it was in the example that programmed Page 1 on a DST token that had the Password Byte programmed. The Write Address, Old Password Byte and new Identifier Byte are in the <*Data Layer*> of the Request Packet. The Password Byte is set to $\mathbf{FF}_{16}$ to represent a token with default Password and the new Identifier Byte for this example is $\mathbf{11}_{16}$.

Request Packet: (**01 0B 00 03 06 65 05 FF 06 96 69**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0B 00	Packet Length 11 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	05	Program Page 1 - Password
Password Byte	FF	Password – Page 1 - Default
Password Value	06	Program Password to 06
BCC	96 69	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 11 06 1A 04 00 05 0D 79 72 8D**)
Validate the data after Password Byte programmed.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	06	Page 1 – Password - 06
Identifier Byte	11	Page 2 – Identifier - 11
MID	06	Page 3 – Man. ID - 06
Serial #	1A 04 00	Page 3 – Serial # - 1050
Read Address	05	Page 1 Write Complete
Token CRC 16	0D 79	CRC 16 on DST packet
BCC	72 8D	LRC and ~LRC

Program DST – Page 3

It is possible to program the data on the Page 3 on the DST transponders as long as that Page has not been locked. The pages cannot be programmed once they have been locked. Page 3 has a single byte of data for the Manufacturer Identifier and three bytes for the token Serial Number. Normally the token manufacturer programs and locks Page 3.

There are two methods of programming Pages 3. The first method does not transmit the Password value to the token. The second method passes the Password value and will only program DST transponders that match that password. The following illustrates how Program Page 3 is accomplished with Password Page not programmed:

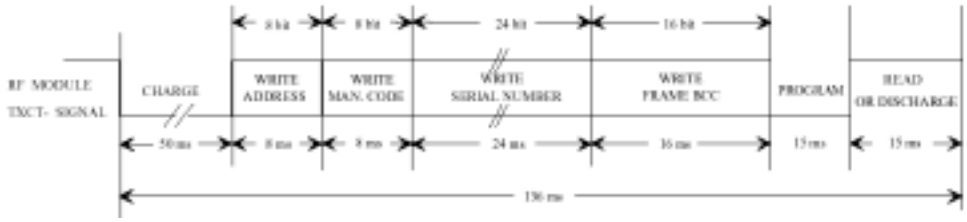

Figure 1-23: Program Page 3 with Password Page Not Programmed

Program Page 3 with the Password Page programmed:

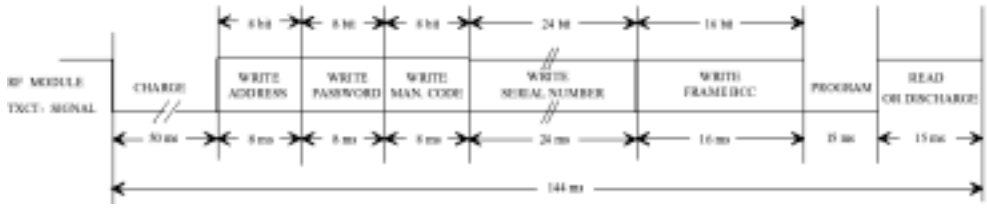

Figure 1-24: Program Page 3 with Password Page Programmed

Both methods calculate a CRC 16 value on the data and transmit it to the token. The CRC value is not passed in the Request Packet. Note that the First method is used when the Password value is the default value $\mathbf{FF}_{16}$. The second method is used when the Password is not set to the default value.

This will require a DST token that has not had its Page Locked. The first diagram is followed when the token Password is the default value $\mathbf{FF}_{16}$. Program Page 3 so that the Manufacture ID Byte is $\mathbf{05}_{16}$ and the token Serial Number is $\mathbf{123456}_{10}$. Note that the Page Address Bits will be $\mathbf{000011}_2$ to point to Page 3 and the Status Bits will be $\mathbf{01}_2$ to indicate a Program instruction. This will require the Write Address to be $\mathbf{0D}_{16}$. The Serial number is sent as three bytes LSB first, so the value $\mathbf{123456}_{10}$ is loaded into the <*Data Layer*> of the Request Packet as $(\mathbf{40\ E2\ 01})_{16}$.

Request Packet: (**01 0E 00 03 06 65 0D FF 05 40 E2 01 3B C4**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0E 00	Packet Length 14 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0D	Program Page 3 – MID, Serial #
Password Byte	FF	Password – Page 1 - Default
MID Byte	05	Program MID to 05
Serial # Bytes	40 E2 01	New Serial # - 123456
BCC	3B C4	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 FF 11 05 40 E2 01 0D F9 F1 53 AC**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	FF	Page 1 – Password - Default
Identifier Byte	11	Page 2 – Identifier - 11
MID	05	Page 3 – Man. ID - 05
Serial #	40 E2 01	Page 3 – Serial # - 123456
Read Address	0D	Page 3 Page Programmed
Token CRC 16	F9 F1	CRC 16 on DST packet
BCC	53 AC	LRC and ~LRC

Repeat the last example but this time the DST Program Page will have been programmed to **06_{16}**.
Request Packet: (**01 0E 00 03 06 65 0D 06 05 40 E2 01 C2 3D**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0E 00	Packet Length 14 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0D	Program Page 3 – MID, Serial #
Password Byte	06	Password – Page 1 - 06
MID Byte	05	Program MID to 05
Serial # Bytes	40 E2 01	New Serial # - 123456
BCC	C2 3D	LRC and ~LRC

Program DST – Page 4

It is possible to program the data on Page 4 of the DST transponder as long as that Page has not been locked. This page cannot be programmed once it has been locked. Page 4 has five bytes for the token Encryption Key. It is not possible to read the data written to Page 4 on a DST token. Issuing a Challenge DST Request can validate the contents of Page 4, but it cannot be read. The Read Byte of the Challenge DST Request will indicate if Page 4 has been locked on the DST token.

There are two methods of programming Page 4. The first method does not transmit the Password value to the token. The second method passes the Password value and will only program DST transponders that match that password.

Program Page 4 with Password Page not programmed:

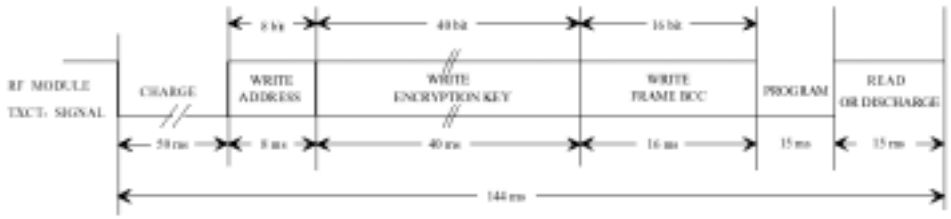

Figure 1-25: Program Page 4 with Password Page Not Programmed

Program Pages 4 with Password Page programmed:

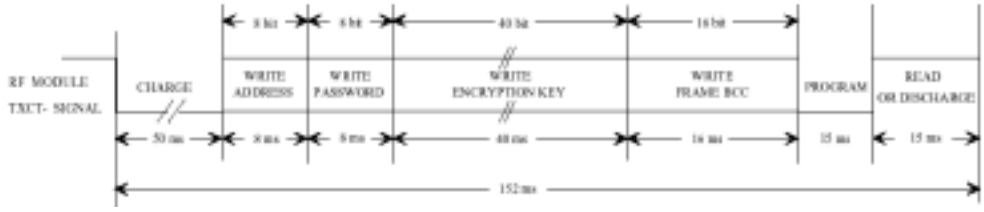

Figure 1-26: Program Page 4 with Password Page Programmed

Both methods will calculate a CRC 16 value on the data and transmit it to the token. The CRC value is not passed in the Request Packet. Note that the First method is used when the Password value is the default value **FF_{16}**. The second method is used when the Password is not set to the default value.

Note the Response Packet has the three-byte token Serial Number and a three-byte Digital Signature. The value returned for the Digital Signature portion of the <*Data Layer*> of the Response Packet is not valid because no encryption is performed during a write.

This will require a DST token that has not had Page 4 Locked. Program the five-byte Encryption Key on a DST token where the Password byte has NOT been programmed and is still default value **FF_{16}**. Program the Encryption Key (Page 4) to the value (**55 44 33 22 11**) $_{16}$. Note that the data is passed in least significant byte first, or (**11 22 33 44 55**) $_{16}$. The Address Bits are set to **000100_2**
Request Packet: (**01 0F 00 03 06 65 11 FF 11 22 33 44 55 91 6E**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0F 00	Packet Length 15 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	11	Program P4 – Encrypt Key
Password Byte	FF	Password – Page 1 - Default
Encrypt Key Bytes	11 22 33 44 55	Encrypt Key - 5544332211
BCC	91 6E	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 1A 04 00 00 00 00 11 3A 3A 03 FC**)
Note that the Read Address Reflects Address Bits for Page 4 and Status Bits reflect Page was
programmed. The Digital Signature is all 0's during a Program Page 4.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Serial Number Bytes	1A 04 00	Token Serial # - 1050
Digital Signature Bytes	00 00 00	Digital Signature – No encryption
Read Address	11	Page 4 Page Programmed
Token CRC 16	3A 3A	CRC 16 on DST packet
BCC	03 FC	LRC and ~LRC

Lock Pages 1, 2, 3, 4

It is possible to Lock Page 1, Page 2, Page 3 or Page 4 on the DST transponders as long as the Pages have not been locked previously. Pages cannot be unlocked once they have been locked.

There are two methods of locking these Pages. The first method does not transmit the Password value to the token. The second method passes the Password value and will only program DST transponders that match this password.

Lock DST Page with Password Page not programmed:

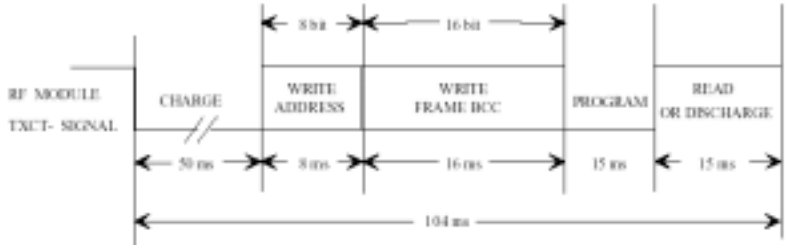

Figure 1-27: Lock DST Page with Password Page not programmed

Lock DST Page with Password Page programmed:

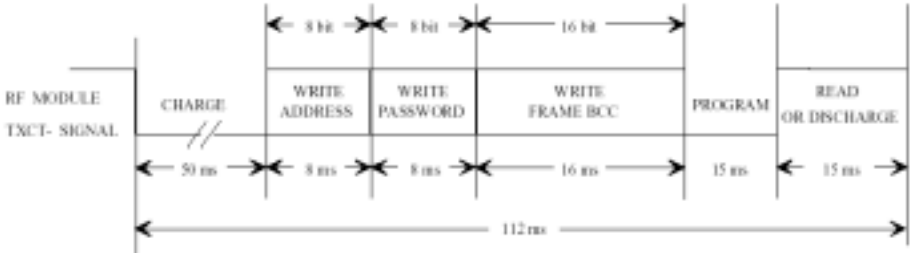

Figure 1-28: Lock DST Page with Password Page programmed

Both methods will calculate a CRC 16 value on the data and transmit it to the token. The CRC value is not passed in the Request Packet. Note that the first method is used when the Password value is the default value $\mathbf{FF}_{16}$. The second method is used when the Password is not set to the default value.

The first example demonstrates how to lock Page 1 on a DST token. This page is the DST Write Password Byte. The <*Data Layer*> of the Request Packet has the Write Address byte followed by the Password byte. The Address Bits is set to $\mathbf{000001}_2$ to point to Page 1 and the Status Bits set to $\mathbf{10}_2$ to reflect a Lock instruction. The Write Address is $\mathbf{06}_{16}$ to lock the Password on Page 1. Note that the Password can never change from this value once it has been locked.
It is possible to lock Page 1 on a DST token that has the default Password by setting the Write Password to $\mathbf{FF}_{16}$. The packet below shows how to lock Page 1 of a DST token with the Password Byte set to $\mathbf{06}_{16}$.

Request Packet: (**01 0A 00 03 06 65 06 06 6B 94**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	06	Lock Page 1 – Password
Password Byte	06	Password – Page 1 - 06
BCC	6B 94	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 06 22 06 BC 04 00 06 9C 69 65 9A**)
Note that the Read Address Page bits point to Page 1 and the Status Bits show Page 1 was locked. The Read Page 1 Request can be used to validate the status of Page 1. Read Address is $\mathbf{04}_{16}$ when unlocked and $\mathbf{06}_{16}$ when locked.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	06	Page 1 – Password - 06
Identifier Byte	22	Page 2 – Identifier - 22
MID Byte	06	Page 3 – MID - 06
Serial Number Bytes	BC 04 00	Token Serial # - 1212
Read Address	06	Page 1 Locked
BCC Bytes	9C 69	DST CRC digits
BCC	65 9A	LRC and ~LRC

This example demonstrates how to lock Page 2 on a DST token. This page is the DST Identifier Byte. The <*Data Layer*> of the Request Packet has the Write Address byte followed by the Password byte. The Address Bits is set to $\mathbf{000010}_2$ to point to Page 2 and the Status Bits are set to $\mathbf{10}_2$ to reflect a Lock instruction. The Write Address is $\mathbf{0A}_{16}$.to Lock the Identifier Byte on Page 2. Note that the Identifier can never change from this value once it has been locked.
It is possible to lock Page 2 on a DST token that has the default Password by setting the Write Password to $\mathbf{FF}_{16}$. The packet below will show how to lock the Page 2 on a DST token with the Password Byte set to $\mathbf{06}_{16}$.

Request Packet: (**01 0A 00 03 06 65 0A FF 9E 61**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0A	Lock Page 2 – Identifier
Password Byte	FF	Password – Page 1 - Default
BCC	9E 61	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E FF 11 06 1A 04 00 0A 92 57 35 CA**)

Note that the Read Address Page bits point to Page 2 and the Status Bits show that Page 2 was locked. The Read Page 2 Request can be used to validate the status of Page 2. Read Address is $\mathbf{08}_{16}$ when Unlocked and $\mathbf{0A}_{16}$ when Locked.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	FF	Page 1 – Password - Default
Identifier Byte	11	Page 2 – Identifier - 11
MID Byte	06	Page 3 – MID - 06
Serial Number Bytes	1A 04 00	Page 3 – Serial # - 1050
Read Address	0A	Page 2 Locked
BCC Bytes	92 57	DST CRC digits
BCC	35 CA	LRC and ~LRC

This example demonstrates how to lock Page 3 on a DST token. This page is the DST Manufacturer ID Byte and Token Serial Number. Note this is normally locked at the manufacturer. The <*Data Layer*> of the Request Packet has the Write Address byte followed by the Password byte. The Address Bits are set to $\mathbf{000011}_2$ to point to Page 3 and the Status Bits set to $\mathbf{10}_2$ to reflect a Lock instruction. The Write Address is $\mathbf{0E}_{16}$ to lock the Manufacturing ID and token Serial Number on Page 3. Note that these can never change from this value once it has been locked.
It is possible to lock Page 3 on a DST token that has the default Password by setting the Write Password to $\mathbf{FF}_{16}$. The packet below shows how to lock Page 3 on a DST token with the Password Byte set to $\mathbf{06}_{16}$.

Request Packet: (**01 0A 00 03 06 65 0E FF 9A 65**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	0E	Lock Page 3 – MID, Serial #
Password Byte	FF	Password – Page 1 - Default
BCC	9A 65	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E FF 11 06 1A 04 00 0E B6 11 53 AC**)
Note that the Read Address Page bits point to Page 3 and the Status Bits show Page 3 was locked. The Read Page 3 Request can be used to validate the status of Page 3. Read Address is $\mathbf{0C}_{16}$ when unlocked and $\mathbf{0E}_{16}$ when locked.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Password Byte	FF	Page 1 – Password - Default
Identifier Byte	11	Page 2 – Identifier - 11
MID Byte	06	Page 3 – MID - 06
Serial Number Bytes	1A 04 00	Page 3 – Serial # - 1050
Read Address	0E	Page 3 Locked
BCC Bytes	B6 11	DST CRC digits
BCC	53 AC	LRC and ~LRC

This example will demonstrate how to lock Page 4 on a DST token. This page is the DST five-byte Encryption Key. The <*Data Layer*> of the Request Packet has the Write Address byte followed by the Password byte. The Address Bits are set to $\mathbf{000100}_2$ to point to Page 4 and the Status Bits set to $\mathbf{10}_2$ to reflect a Lock instruction. The Write Address is $\mathbf{12}_{16}$ to lock the Encryption Key on Page 4. Note that the Encryption Key can never change from this value once it has been locked. It is possible to lock Page 4 on a DST token that has the default Password by setting the Write Password to $\mathbf{FF}_{16}$. The packet below will show how to lock the Page 4 on a DST token with the Password Byte set to $\mathbf{06}_{16}$.

Request Packet: (**01 0A 00 03 06 65 12 FF 86 79**)

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	0A 00	Packet Length 10 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST Request
Write Address	12	Lock Page 4 – Encrypt Key
Password Byte	FF	Password – Page 1 - Default
BCC	86 79	LRC and ~LRC

Response Packet: (**01 13 00 03 06 65 00 7E 1A 04 00 00 00 00 12 A1 08 A9 56**)

Note that the Read Address Page bits point to Page 4 and the Status Bits show Page 4 was locked. The Digital Signature is all 0's during a Lock Page 4. The Challenge DST Request can be used to validate the status of Page 4. Read Address is **10_{16}** when unlocked and **12** $_{16}$when locked.

Field	Contents	Summary
SOF	01	Start of Frame
Packet Length	13 00	Packet Length 19 bytes
Device ID	03	Terminal is MFR
Command 1	06	LF DST Layer
Command 2	65	Write DST
Status Byte	00	ERROR_NONE
SOF	7E	Start of Frame
Serial Number Bytes	1A 04 00	Token Serial # - 1050
Digital Signature Bytes	00 00 00	Digital Signature – No encryption
Read Address	12	Page 4 Locked
Token CRC 16	A1 08	CRC 16 on DST packet
BCC	A9 56	LRC and ~LRC

Write DST Function Table

The following table outlines the valid Write Addresses for the Write DST function. Some additional information will help determine Request Packet Data field contents. All values shown are in Hex. **N/A** represents password not applicable, **XX** represents a case where the token password would be required in Request Packet. Note that **FF_{16}** should be inserted in a situation where a password is required, but the password page has not been programmed in the transponder. **L** represents Locked and **UL** represents unlocked transponder page. **PP** represents Program Page. Note multiple byte fields are LSB first.

Write Addr.	Instruction	Password Byte	Additional data required in the Request Packet	Read Address Returned
04	Gen. Read Page 1	N/A	None	04 = UL; 06 =L
08	Gen. Read Page 2	N/A	None	08 = UL; 0A=L
0C	Gen. Read Page 2	N/A	None	0C = UL; 0E =L
07	Sel. Read Page 1	XX	None	04 = UL; 06 =L
0B	Sel. Read Page 2	XX	None	08 = UL; 0A =L
0F	Sel. Read Page 3	XX	None	0C = UL; 0E =L
05	Write Page 1	XX	1-byte Password	05 = PP
09	Write Page 2	XX	1-byte Identifier	09 = PP
0D	Write Page 3	XX	1-byte MID; 3-byte Ser #	0D = PP
11	Write Page 4	XX	5-byte Encrypt Key	11 = PP
06	Lock Page 1	XX	None	06 = L
0A	Lock Page 2	XX	None	0A = L
0E	Lock Page 3	XX	None	0E= L
12	Lock Page 4	XX	None	12 = L
10	Gen. Encrypt	N/A	5-byte Random Number	N/A
13	Sel. Encrypt	XX	5-byte Random Number	N/A

Figure 1-29: Write DST Function Table

Chapter 2

Regulatory and Warranty Notices

Topic **Page**

2.1 FCC Conformity

The Series 4000 Multi-Function Reader is an intentional radiator. The transmitter portion operates at 13.56 MHz and is subject to FCC Part 15, Subpart C, “Intentional Radiator,” paragraph 15.225 (13.553-13.567MHz). Radiated emissions from the device are subject to the limits in Section 15.209 of the Rules outside of the 13.56 +/- 0.007 MHz band.

Note:

Any device or system incorporating the Series 4000 reader, in full or in part, needs to obtain FCC certification as part of the system within which this reader unit resides. A system containing this product may be operated only under an experimental license or final approval issued by the relevant approval authority. Before any such device or system can be marketed, an equipment authorization must be obtained form the relevant approval authority.

2.2 ETSI Conformity

Any device or system incorporating the Series 4000 reader, in full or in part, may need to comply with European Standard EN300330. It is the responsibility of each system integrator to have their complete system tested and to obtain approvals as required from the local authorities before operating or selling this system.

2.3 CE Conformity

Any device or system incorporating the Series 4000 reader, in full or in part, may need to have a CE Declaration of Conformity stating that it meets European EMC directive 99/5/EC. This must be issued by the system integrator or user of such a system prior to marketing or operating it in the European community.

2.4 Warranty and Liability

The "General Conditions of Sale and Delivery" of Texas Instruments Incorporated or a TI subsidiary apply. Warranty and liability claims for defect products, injuries to persons and property damages are void if they are the result of one or more of the following causes:

- Improper use of the reader module.
- Unauthorized assembly, operation and maintenance of the reader module.
- Operation of the reader modules with defective and/or non-functioning safety and protective equipment.
- Failure to observe the instructions during transport, storage, assembly, operation, maintenance and setting up of the reader modules.
- Unauthorized changes to the reader modules.
- Insufficient monitoring of the reader modules' operation or environmental conditions.
- Improperly conducted repairs.
- Catastrophes caused by foreign bodies and acts of God.