M.O.S.T. Toolz

Microprocessor Card Development Kit

User Guide

CardLogix

PUBLICATION NOTICES

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of CardLogix Corporation. CardLogix Corporation shall not be held liable for technical and editorial omissions or errors made herein; not for incidental, or consequential damages resulting from the furnishing, performance or use of this material. CardLogix Corporation reserves the right to revise this publication and to make changes from time to time in its content without obligation of CardLogix Corporation to notify any person or organization of such revision or change.

Trademarks

M.O.S.T. Toolz™ is a trademark of CardLogix Corporation. Winplex®, Printplex®, CardAppz™, Smart Toolz®, and idblox® are are registered marks of CardLogix Corporation. All terms used in this document that are known to be trademarks or service marks have been capitalized where appropriate. CardLogix Corporation cannot attest to the accuracy of this information. Use of a term should not be regarded as affecting the validity of any trademark or service mark.

General Notice

Some of the product names used herein have been used for identification purposes only and may be trademarks of their respective companies. Microsoft Windows XP, and Vista are all registered trademarks of the Microsoft Corporation.

FCC

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment has been certified to comply with the limits for a class B computing device, pursuant to FCC rules.

Statement of Electromagnetic Compliance

This product has passed all electromagnetic interference and susceptibility testing required by the European Community and thus bears the "CE" mark.

- This product has passed all electromagnetic interference and susceptibility testing required by the European Community and thus bears the "CE" mark.
- This Class B Digital Apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

LICENSE AGREEMENT

Software License Agreement and Hardware Agreement for M.O.S.T. Toolz Development Kit

This agreement is made by and between you (either an individual or an entity) and CardLogix Corporation.

By opening this sealed package and/or by installing and using the product, you are agreeing to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, promptly return the product (retaining no copies) to the place that you obtained it from for a refund.

Title

Subject to any rights deriving from any patent (either registered, pending, or that can be registered). CardLogix and/or any third party hold or shall hold in the hardware (i.e. all the tangible elements of the product) or any part thereof. CardLogix sells you the hardware.

The software contained in the product (including any revisions, improvements, and/or updates) and related documentation (necessary and/or related to the use of the product, in hard copy and/or electronic form) is not for sale; title in and to the software and documentation shall remain solely with CardLogix.

License

CardLogix grants you a non-exclusive right to use the product for the sole purposes of developing smart cards and smart card applications based exclusively on CardLogix cards. The software and documentation shall not be used for any other purposes.

You are permitted to make one (1) copy of the software solely for development and backup purposes.

You may alter, merge, modify, or adapt the Winplex software but only in order to "and to the extent required" merge it with your smart card application. You may not disassemble and/or decompile and/or reverse engineer the software or any part thereof. You have a royalty-free right to reproduce and distribute binary executable files which include some or all of the Winplex software, only in binary executable form, provided that the binary executable files do not constitute an application that may compete and/or imitate and/or substitute the software. The media containing the binary executable files displays your copyright notice, and the title page or title page version of the documentation which accompanies the binary executable files must contain the following CardLogix copyright notice:

"Portions Copyright © 1997-2014, CardLogix Corporation. All rights reserved."

Within forty-five (45) days of your first transfer or shipment of said application to a third party, you shall send CardLogix a copy of the CD label or title page containing the CardLogix copyright notice specified above. CardLogix will acknowledge receipt of this copy. In the event that you cannot satisfy the conditions of the above paragraph, contact CardLogix regarding an amendment to this agreement. You may not rent, lease, loan, or sub-license the product or any part thereof. You may not transfer your rights under this agreement to any party. Apart from the right of use explicitly granted herein, you shall have no other rights, express or implied, in the software.

Proprietary Right

All intellectual property rights in the software and documentation and some of the intellectual property rights in the hardware are owned by CardLogix and are protected by its copyright, patent, trademark, trade name and trade secret laws, and international treaty provisions. You agree that the software is the proprietary property of CardLogix and that it is distributed subject to restricted disclosure only and that the license does not convey to you an interest in or to the software, but only grants you a limited right of use in accordance with the terms of this agreement.

The hardware is provided "as is" and CardLogix shall have no liability to you for the infringement of any patents, copyrights, trade secrets or other proprietary right by the hardware or any portion thereof.

Limited Warranty and Limitation of Liability

CardLogix warrants that (a) the software will perform substantially in accordance with the accompanying user documentation for a period of one (1) year from the date of receipt and (b) that the hardware, under normal use and service, is free from defects in materials and workmanship for a period of one (1) year from the date of receipt. Any implied materials and workmanship are warranted for a period of one (1) year from the date of receipt. Any implied warranties on the software and hardware are limited to one (1) year, respectively. The foregoing warranty shall not apply to consumable portions of the hardware which are expendable by nature. Some states/jurisdictions do not allow limitations on duration of an implied warranty.

CardLogix' entire liability and your exclusive remedy shall be at CardLogix' option for either (a) refund of the price paid or (b) repair or replacement of the software or defective hardware that does not meet CardLogix' limited warranty, if returned to CardLogix, with a copy of your receipt, within 90 days of the date of receipt. This limited warranty is void if failure of the software or defective hardware has resulted from: (i) accident, abuse or misapplication and/or modifications are made to the product by anyone other than CardLogix; (ii) attachments, features or devices that are employed on the hardware which are not supplied by CardLogix or not approved for use, in writing, by CardLogix; (iii) or other than the current version of the software available from CardLogix is used on the hardware. The warranty and remedies set forth herein are exclusive and in lieu of all others, oral or written, express or implied. No CardLogix dealer, distributor, agent or employee is authorized to make any modification or addition to this warranty, save that nothing in it affects any rights you may have against us for death or personal injury caused by our negligence.

Except for and to the extent expressly provided herein, CardLogix makes no warranty or representation, either expressed or implied, with respect to the product, including its quality, performance, merchantability or fitness for a particular purpose.

Please note that the software is inherently complex and may not be completely free of errors. To the degree permitted by applicable law, in no event shall CardLogix be liable for direct, indirect, special, incidental, consequential or any other damage whatsoever (including, without limitation, damages for loss of business information or other pecuniary loss) arising out of or related to this agreement or the performance or breach of CardLogix' liability and/or the use of or inability to use the product, even if CardLogix has been advised of the possibility of such damages. In no case shall CardLogix' liability under any provision of this agreement exceed the amount actually paid by you for the product. To the extent that applicable law does not allow the exclusion or limitation of implied warranties or limitation of liability for incidental or consequential damages, the above limitation or exclusion may not apply to you.

General

This agreement is governed only by the laws of the State of California and only the courts in California shall have jurisdiction in any conflict or dispute arising out of this agreement.

Any cause of action arising out of or related to this agreement must be brought by you no later than one (1) year after the cause of action has occurred.

This license agreement is effective upon your opening the accompanying package and shall continue until terminated. You may terminate this license agreement at any time. Upon the breach by you of any term or condition of this license agreement, and any subsequent failure to correct the breach within fourteen days of notification of the breach, CardLogix may terminate this license agreement. Upon termination of this license agreement by you or CardLogix, you agree to immediately return the software to CardLogix, to continue to maintain the software confidential, and to immediately destroy all copies of the software, whether in whole or in part, whether modified or not, whether in source object or binary executable form.

Copyright

Disclaimer

Although CardLogix endeavors to ensure the best possible product quality, CardLogix does not warrant that the M.O.S.T. Toolz software will function properly in every hardware and software environment. The M.O.S.T. Toolz software may not work in combination with some networks and some programs. It may not work with modified versions of the operating system or with specific patches. The M.O.S.T.Toolz software may not function properly with certain modems and/or certain printers. Not all supported devices will work with all operating systems.

TABLE OF CONTENTS

Publication Notices 1

License Agreement... 3

Section I: Introduction.. 9

How to Use This Manual 9

Section II: Getting Started 11

Check the Contents of Your M.O.S.T. Toolz™ Kit 11

Installing M.O.S.T. Toolz™...11

Troubleshooting...11

Returns...12

Section III: M.O.S.T Card® Architecture & Overview......... 13

Smart Card Communication 13

Memory 15

Program Memory/ROM Functions..15

M.O.S.T. Toolz™ File Structures..15

Files and Identifiers 17

EF and Purse File Protections...17

Linear and Cyclic EFs..17

Key Management...19

Transport Keys 21

Administrator Keys 21

Injectable AES Keys 21

HMAC Keys 22

Verifying Your Cards 22

Section IV: The M.O.S.T. Card® Development Process...... 23

M.O.S.T. Toolz™ and Winplex©.. 23

Selecting a Card Type 24

Pre-Production File System Development Process 24

Create and Configure the File System 25

Limited Life Demo Smart Cards with a Test File System 26

Obtain Production Check Smart Cards 26

Test and Validate Production Check Smart Cards 26

Card Artwork & Personalization...27

Section V: M.O.S.T. Toolz™ Software Overview................. 29
Installing the Software..29
Running the M.O.S.T. Toolz™ File Creation Utility 29
Using the M.O.S.T. Toolz™ Card Configuration Utility 30
Using idblox® files with M.O.S.T. Toolz 31
Creating a Custom Card File Structure...33
Setting the File Properties 33
DF Files..33
Transparent Files 34
The Transparent File Editor...36
Write Fill Character 38
Purse Files 38
CHV Files..40
APP Files 41
Writing to a Limited Life Card...42
DES Keys...42
HASH IDs 43
Viewing Information About the Current Card...................................44
M.O.S.T. Toolz Program Menu Command Summary 45
Section VI: Accessing the Card without Using Winplex®. 49
Microsoft PC/SC API 49
Appendix A: System Deployment Recommendations..... 51
Appendix B: Programming Notes 53
Appendix C: Glossary 55

SECTION I: INTRODUCTION

Welcome to M.O.S.T. Toolz™, the easiest to use Smart Card Development Kit. With this kit, you will find everything you need to build a smart card for your system and then test your ideas. The items included in the kit are production items and may be purchased in volume from CardLogix®.

The design environment serves two functions: setting up the files, and configuring a M.O.S.T. Card®. The setup includes all the formatting and permissions for each file that will be on the card. After the set up is completed, the included Winplex® middleware will enable you to easily make function calls to the card from your VB, C++, or C# application.

If you are building a stored value system that will require a wide distribution of cards, please call CardLogix® sales at (949) 380-1312 to discuss the specific issues relating to printing, terminals, security and card and key issuance.

How to Use This Manual

The CardLogix® M.O.S.T. Toolz™ User Manual is designed to help you install your M.O.S.T. Toolz™ as quickly and efficiently as possible. Each chapter includes simple explanations and easy-to-follow steps that will help you understand the installation and functions of your M.O.S.T. Toolz™ kit. This guide assumes familiarity with windows based programming terms and environments as well as a complete knowledge of the hardware used in working with your development.

- **Section II: Getting Started** – Provides information about your M.O.S.T. Toolz kit. Included in the kit are the installation instructions and your Warranty Registration Card.
- **Section III: M.O.S.T. Toolz™ Card Architecture & Overview** – An explanation of how CardLogix M.O.S.T. Cards function and are designed, as well as implementation of a card system with CardAppz™. This is recommended reading if you have no programming experience.
- **Section IV: M.O.S.T. Card® Development Process** – Describes how to develop your smart card program using the CardLogix M.O.S.T. Cards that have been included in your development kit.
- **Section V: M.O.S.T. Toolz™ Software Overview** – Describes how to install and use the M.O.S.T. Toolz™ Microprocessor Card Development Kit software.
- **Section VI: Accessing the Card Without Using Winplex®** – Describes how to access the card if your card is being deployed into a non-Windows environment, using low-level APDU commands. These commands follow the ISO 7816 specification.
- **Appendix A: System Deployment Recommendations** – This section describes the steps we recommend for a profitable and successful card project.
- **Appendix B: Programmer's Notes** – This section is written to assist you with the special programming requirements for working with Smart Cards.
- **Appendix C: Glossary** – This section lists commonly used terms in the smart card industry.

SECTION II: GETTING STARTED

Check the Contents of Your M.O.S.T. Toolz™ Kit

Carefully remove the contents of the M.O.S.T. Toolz kit. To protect your kit when in storage, save the box and all packaging materials.

- ☑ Software License Agreement
- ☑ Smart card reader/writer
- ☑ CD containing software, PDF documentation and examples
- ☑ User guide
- ☑ 10 M.O.S.T. CardLogix sample cards, and technical briefs on each
- ☑ CardLogix Warranty Registration Card
- ☑ Customized Technical Data Sheet for development CPU Cards

Installing M.O.S.T. Toolz™

1. Make sure to read and accept the terms of the License Agreement.
2. Start Windows.
3. Insert the program CD into your CD-ROM drive.
4. The M.O.S.T. Toolz install wizard should start automatically. If it does not, browse to your CD File Location and start the installation wizard manually by double-clicking on Menu.exe.
5. Follow the on-screen instructions.

The setup program will copy the required files to your system and create the necessary program groups. To relocate the Winplex® API in another location, go to the CardToolz™ installation directory, click on the individual folder, and move the DLL's to your working location.

Troubleshooting

If you are experiencing difficulty with any of the M.O.S.T. Toolz software or hardware please contact us at www.cardlogix.com/corporate/contact.asp or send an e-mail to sales@cardlogix.com describing the problem.

When contacting us regarding problems please make sure you have the following information available:

1. The toolkit serial number (found on side of your box).
2. Your operating system and system components.
3. The card part number (P/N) that is being used.
4. Complete details of the problems that you are experiencing, with references to any errors, if available.

The M.O.S.T. Toolz™ Warranty covers only functional defects, not implementation difficulty!

Returns

Please contact CardLogix regarding any and all merchandise that is not performing to the published specifications. In the event of a defect in material or workmanship during the warranty period, CardLogix, at its discretion, will repair or replace the defective product after it is returned to CardLogix by the owner.

For return of product, you must be issued, by CardLogix, a Return Material Authorization (RMA) number. We cannot issue an RMA Number unless you have registered your system. This RMA Number is to be included in any returned merchandise. Please mark the RMA Number on the shipping box and on the packing slip.

You are responsible for the shipping charges when returning items to CardLogix for quality review. If the items are found to be defective and within the warranty terms and/or period, CardLogix will pay for all shipping charges (company policy is UPS 2nd day air) to return the required device(s) to you.

SECTION III: M.O.S.T CARD® ARCHITECTURE & OVERVIEW

The M.O.S.T. Card® family of smart cards is based on 8-, 16-, and 32-bit microcontroller chip technology, which consists of the following functional blocks:

- CPU/processing capability
- Input/output capability
- Program memory/ROM
- User memory/EEPROM.

Each chip contains a clock that is responsible for pacing the CPU when it:

- Manipulates data
- Interprets data
- Executes program memory instructions

All M.O.S.T. Cards contain a random number generator, which is used for authentication and symmetric key cryptography. For a more detailed description of each M.O.S.T. Card, please ensure that you have obtained the appropriate specification for the card you are using. All M.O.S.T. Cards utilize the same command structures but differ in some areas of functionality and memory size. Each M.O.S.T. Card Type will have a different ATR.

Smart Card Communication

For power and communications with its environment, the M.O.S.T. Card employs:

- Metallic interface contacts on the card's surface
- ISO 7816 T=0 protocols and or ISO 14443 contactless protocol
- A card reader protocol API (See the WinPlex® card reader DLL)
- Card contact landings (for cards with a contact chip)

There are eight metallic contact pads on the surface of the M.O.S.T.™ card. When the card is inserted into a card reader, power is sent through these contacts to the card chip, which is embedded in the card. One of these contacts is used for serial communication of the data. The device is first reset, and then begins to execute its Card Operating System (COS) commands and operating system extensions with an Answer to Reset (ATR). For more information on the ATR please refer to the CardLogix ATR Definitions document, found in your M.O.S.T. card specification.

To better understand the card interface contacts, refer to the ISO specification or contact CardLogix for a Technical Brief.

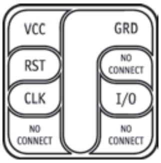


Figure 3.1 *- A typical smart card module.*

Contactless M.O.S.T. cards operate at 13.56 MHz. The cards communicate with readers and terminals through inductive coupling between the reader/terminal antenna and the card antenna. They are also powered by this method.

Contactless Reader/Terminal
Contactless M.O.S.T. Card
M.O.S.T. CARD
Microprocessor Operating System Technology
CardLogix

Figure 3.2 *- Contactless M.O.S.T. Card communication.*

An alternating magnetic field is produced by a sinusoidal current that flows through the reader/terminal antenna loop. When the card enters the alternating magnetic field, an alternating current (AC) is induced in the card antenna loop. The card's integrated circuit converts AC to direct current (DC), which powers the integrated circuit.

By modulating its RF field, the reader/terminal is able to send information to the card. The card's smart chip then converts the reader's amplitude modulation into a digital signal.

Memory

The M.O.S.T. Card memory consists of:

- Program memory/ROM (Read Only Memory): The COS is embedded in ROM at the time of manufacture. The COS controls card functions through the program memory and cannot be altered, except by CardLogix.
- RAM (Random Access Memory): Serves as temporary data storage for use by the COS.
- User memory/EEPROM (Electrical Erasable Programmable Read Only Memory): Stores primary customer file data and has files for specific functions and commands. The general commands are pre-configured, but the data connected with each is loaded and updated by the card issuer.

Program Memory/ROM Functions

The ROM performs the following functions:

- The ROM-resident COS administers the access security system.
- Input / output handling
- Reset control
- Data transfer protocol
- Command interpretation routines and extensions. This includes all global commands that are supported by the Smart Card (PC/SC).
- Data and directory administration. The ROM-resident COS manages the directories and data contained in the User memory/EEPROM.

M.O.S.T. Toolz™ File Structures

Data on the M.O.S.T. card is stored in a series of files. These files are organized in a simplified tree structure similar to that found on your PC's hard drive. Each card should contain a Master File (MF), Directory Files (DFs), and simple files. The simple files are used to hold card data and control access to the data files. A M.O.S.T. Card can contain the following file types:

Master File (MF)

There is only one Master Files in each card file structure. The information that it contains is fixed and cannot be modified. A Master File can be considered as the file system's "root directory".

Dedicated File Directories (DFs)

DFs contain groups of files and can be used to organize similar files in a single location. This file acts as an umbrella for security functions for a specific set of data (e.g. transactions). A card file structure may contain multiple DFs. DFs cannot contain other DFs. They are sometimes referred to as "Application Directories" or "AIDs".

Elementary Files (EFs)

EFs store user or system data and may be used to store sensitive data. Access to EFs can be controlled by Password Files or Authentication Files. EFs can also have their data encrypted for additional security. They are sometimes referred to as "Data Files".

The CardLogix C-Series cards support three types of EF types: transparent, linear, and cyclic. Transparent EFs are typically used for normal binary data. Linear and cyclic EFs are used to store certain data, such as transactions, sequentially. A linear file holds a preset number of records that have to be erased to provide additional space in the file. This behavior is different with a cyclic file where, after a preset number of records are reached, the write function overwrites the oldest record.

Purse Files

Purse Files are sophisticated files that are designed to securely store value. Access to these files can be controlled by Password Files or Authentication Files. They can also have their data encrypted for additional security.

Password Files (CHVs)

Password Files are simple files that can store a password or PIN. They are used to control access to EFs and Purse Files. CHVs typically contain a password or PIN known only by the user or the system that interacts with the card. A user of the card may be able to change the code.

Global Password File (GPF)

There can only one Global Password File in each card file structure. GPFs can be used to restrict the ability of the card operating system to select any file. If a GPF is present and active, the card will be unusable until either the correct password/PIN is given or the GPF is reset by the issuer in order to unblock the card. The GPF may only be blocked or unblocked by the issuer.

The GPF value may be changed after a verify command is successfully is performed with the administrator key. This file is often made available to the individual user to set for personal card control.

Authentication Files (APPs)

Authentication Files are simple files that contain authentication data and are used to control access to Elementary Files and Purse Files. APPs contain a password that is known by the creator of the card, but not the user. This password is typically common for all cards and cannot be modified by the user. APPs are used by card applications to prove their authenticity to the card. The M.O.S.T. C-Series cards uses SHA-1 and SHA-256 for internal and external authentication functions.

Files and Identifiers

All files on a M.O.S.T. Card are identified by a two-byte identifier. The C7, C8, C9, and C10 family of cards also support long file names. The following information explains the different rules for file identifiers (the byte values are represented in hexadecimal):

- The Master File ID is 3F00
- The values 2000-2FFF, 3FFF, and FFFF are reserved
- The first byte for a DF file may range from 10 to EF. The second byte of a DF is 00.
- The first byte of an EF or Purse must be the same as the first byte of the DF it is defined under. The second byte may range from 40 to 5F. This allows you to define up to 32 EFs and Purses in a single DF.
- The first byte of a CHV must be the same as the first byte of the DF it is defined under. The second byte may range from 80 to 8F. This allows you to define up to 16 CHVs in a single DF.
- The first byte of an APP must be the same as the first byte of the DF it is defined under. The second byte may range from 90 to 9F. This allows you to define up to 16 APPs in a single DF.

EF and Purse File Protections

As stated earlier, EF and Purse files may have access restrictions. The file system supports controlling Read, Write, Update, Invalidate, and Rehabilitate access to a file through the use of CHV and APP files. To gain access to a feature for a file, you must first present the correct authentication for that feature. By default, there are no access restrictions on a file. However, you are strongly urged to place restrictions on your data. For each feature, access can be defined as:

- Unrestricted - No authentication needed for access.
- APP Restricted – Access to the file is forbidden until the associated APP has been authenticated.
- CHV Restricted – Access to the file is forbidden until the associated CHV has been verified.
- Completely Restricted – Access is permanently disallowed (for example, you may not want to allow a file to ever be Rehabilitated).

The CHV or APP files used to restrict a file must either exist in the same DF as the file or in the MF. For example, the file 3D40 could be protected by the CHV 3D80 or 3F80, but not by the CHV 3E80.

Linear and Cyclic EFs

Linear and cyclic EFs are designed for structured record-keeping functions like the ones commonly used in financial transactions, voting, and machine-to-machine applications. Each file type behaves in a similar fashion. However, in a cyclic file, after a preset number of records are reached, the write function will begin overwriting the oldest record.

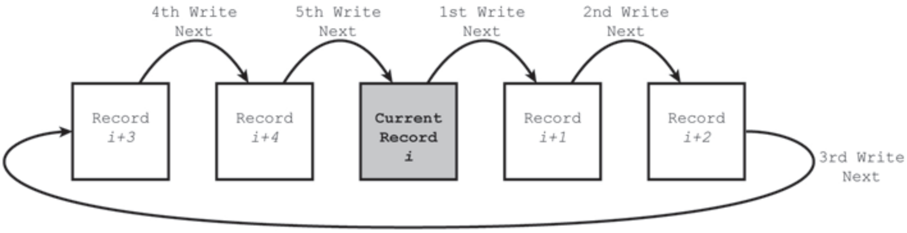


Figure 3.3 *- Example of writing to a Cyclic File with 5 records. Each write command is performed on the next available record. When all records have been written to, the oldest record is overwritten, starting the cycle over once again.*

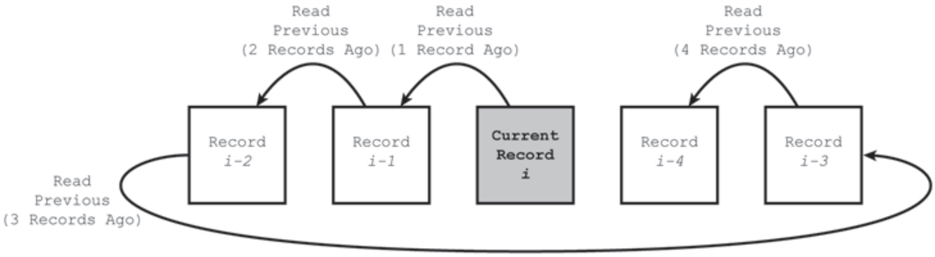


Figure 3.4 *- Example of reading from a Cyclic File with 5 records. All record references use the current record as a starting point. In a set of* n *records, the last* n-1 *previous records are available for reading.*

Cyclic Files can be considered as a looped buffer of records that are selected and accessed as a single file. With each consecutive write operations, the next adjacent record is used. This design allows write and erase operations to be spread across a larger area of EEPROM.

This file architecture helps preserve the EEPROM by reducing the effective wear on a specific memory cell through consecutive write and erase procedures. (M.O.S.T. Cards support 250,000 write/erase cycles per EEPROM cell).

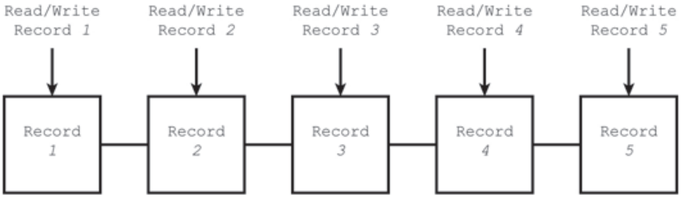


Figure 3.5 *- Example of a Linear File with 5 records. Each file is accessed directly.*

Linear Files consist of a set of records, ranging from 1 to 254 bytes in length. The maximum number of Linear File records is 254. Records in Linear Files are fixed in length. Records in Linear Files are accessed directly using the record number, given to your command as a parameter. This can be done at a low level with a formed APDU command to the card. Alternatively, the programmer may choose to use a Winplex API call. Note that the write command only works if the data in the record is blank (all 0xFF). To overwrite existing data, the programmer must use the `UPDATE_RECORD` command at the APDU level or the `CLX_LinearRecordUpdate` command in the Winplex DLL.

The access functions for Cyclic and Linear Files are further detailed in each specification for M.O.S.T. Cards that support these file types. API command documentation, complete with example source code, is available in the *Winplex Programmer Guide*.

Key Management

Keys are values stored securely in the card. The same (symmetric) keys also need to be securely stored in the host computer, terminal, or Physical Access Control System (PACS). If you are using an idblox file template, you can only change the keys and part of the file name. This ensures that the corresponding idblox application suppliers will know where to look for the data.

The keys generated in the M.O.S.T. Toolz CFS can enable a multitude of secure functions that the card might execute in conjunction with a corresponding application. Keys are used for authentication, encryption, and data integrity functions with signature delivery of a message. They are also used to control user permissions for password changes. After a CFS is finalized, it is important to export the file map to a secured document for your own reference. This is done through the export function (to a .csv or .xls file). Due to the fact that keys are often long and can be prone to errors if manually entered, we suggest that you cut and paste them into a secured electronic document before sharing them with the corresponding application provider. This exchange is often referred to as a “key ceremony” and typically involves an encrypted delivery method (e.g. PGP).

Table 3.1 - M.O.S.T. C-Series key types.

Key Type	Suggested Use or Function	Quantity	Length (Bytes)	C5	C6	C7	C8	C9	C10	Reset-table
Transport	Moving the whole card through lifecycles	2	16 or 32	✓	✓	✓	✓	✓	✓	✓
Administrator	Secure changing of other keys	1	16		✓	✓	✓	✓	✓	
Global Password	PIN for Card	1	8		✓	✓	✓	✓	✓	✓
Injectable AES Key	Access Control Systems	3	16		✓	✓	✓	✓	✓	✓
AES	General Data Protection	3	32	✓	✓	✓	✓	✓	✓	
DES	General Data Protection	3	8	✓	✓	✓	✓	✓	✓	
HMAC	To insure data integrity and to identify the sender	3	64			✓	✓	✓	✓	

Keys are designed so that they cannot to be extracted from a card's chip memory. The symmetric nature of the algorithms that utilize these keys demands extreme care on both ends of a system to ensure system wide security.

The keys are often used as a seed, with a random number generated by the card or host, to make session keys. These keys are only used once to transmit data across a card-to-reader connection and are never used again. By using session keys, the original keys are never revealed. This protects the value or data that is transmitted from being discovered through replay attacks or reverse engineering.

It is prudent to assume that potential hackers are familiar with the cryptographic algorithms for your system and card. Keys should be chosen and managed with care to prevent attacks using common techniques.

Think of keys as the combination to your safe. For more information on key management we recommend the publication at the following URL as a guideline:

`http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.`

At a minimum, the transmission of keys across the Internet must be protected by a secure methodology such as PGP.

Transport Keys

Transport Keys are now standard on all C-Series M.O.S.T. Cards. They give the card system designer a mechanism to change access permissions to the card as it moves through the lifecycles that are typical for payment and ID cards. For example, a card may be issued but remain inactive until specific actions are performed at a terminal. In this case, a terminal's application software can be programmed to read the card and determine if activation is appropriate. The functionality is optional and is typically controlled by a Card Management System (CMS) or a pre-planned set of key change operations, which are based on the state of the card in its intended life cycle. For more information on these keys and functions, please refer to your card's specification document.

Table 3.2 – Transport Key life cycle states (examples).

Life Cycle State	Cards leaving the CardLogix factory	Cards that are personalized at issuer site and are ready for pickup	Cards that are issued to the end user	System shutdown of a card, based on a security flag	Re-activated card, based on a cleared security flag
Customer Defined Key Set	1	2	3	4	5

Administrator Keys

An Administrator Key is a 32-byte AES password that cannot be read or modified by a user. Authentication is performed with a challenge/response exchange directly between the card and terminal. A retry counter is used to prevent multiple unsuccessful attempts. The Administrator Key must be set in M.O.S.T. Toolz and is permanently installed when the CardLogix initializes the card.

Injectable AES Keys

Injectable AES Keys have values that may be changed after successful authentication with the Administrator Key. They are designed to be used for access control or transaction terminal update functions. Refer to `CLX_ChangeInjectableAESKey` in the Winplex Programmer Guide for more information.

HMAC Keys

HMAC Keys are each 64 bytes in length and are used to execute Hash Message Authentication Code (HMAC) functions. The HMAC function, specified by NIST FIPS PUB 198.1, ensures the accurate delivery of a message or a data package by comparing the HMAC Key of the data at its source and the key of the data at its destination. Note that the secure use of this function requires a Key Management System that works with HMAC keys. Refer to `CLX_SignMessage` and `CLX_VerifyMessage` in the Winplex Programmer's Guide for more information.

> ***Warning:*** If you lose or forget your password, it cannot be recovered and you will not be able to open your card. ***There is absolutely no way for you or our programmers to retrieve your password.*** Please keep a record of your passwords and their databases in a safe place.

Verifying Your Cards

The card structure of any CardLogix card can be verified by the use of M.O.S.T. Toolz. File Creation Limited Life Development Cards have been designed with a very limited life of 150 power on reset cycles, (this is for an added layer of security). See the M.O.S.T. Toolz Software Overview for more information about programming the file structure onto a card.

Additional cards are available from CardLogix at a nominal cost.

SECTION IV: THE M.O.S.T. CARD® DEVELOPMENT PROCESS

M.O.S.T. Toolz™ and Winplex©

M.O.S.T. Toolz™ ships with two powerful sets of software, the M.O.S.T. Toolz Card Configuration Utility and the Winplex© API. After designing your data workflow, you can use them to get to market faster.

The Winplex API/DLL may be used in your application, royalty-free. It will allow you to perform many complex security functions without having to perform any low-level programming. It will also help managing card reader functionality in your system. The Winplex API demonstration console, included in with M.O.S.T. Toolz, lets you view each command in detail with accompanying source code.

Table 4.1 - M.O.S.T. Toolz Card Configuration Utility and Winplex API/DLL usage.

M.O.S.T. Toolz Card Configuration Utility	WInplex API/DLL
Used for developing Card File Structures.	Used for developing card software applications.
Software for configuring logical data structures security keys and settings for cards.	API/DLL for software application development that contains commands for working with specific data files and their keys on cards.

Each M.O.S.T. Toolz kit comes with a variety of M.O.S.T. Cards. They are designed to help you quickly understand each specific function of the CardLogix product offerings.

Some cards are permanently locked with a file structure. These cards are designed to demonstrate many of the functions of M.O.S.T.™ Cards, and to build your understanding of the CardLogix M.O.S.T.™ Card product. They can be accessed through the included demonstration source code found in the Winplex® API examples. By using these cards to inspect your hardware setup and software installation, you will be able to get an ATR and utilize card file protection mechanisms such as PINs (CHVs), authentication (APPs), and encryption (AES). When you are ready to start your own file system development, the limited life cards can be configured with your specific card file structure (CFS).

Selecting a Card Type

The selection of a card type requires a baseline knowledge of how the card is to be used with your application. It is assumed that a program or application specification is either complete or in progress. Armed with this definition of how the application will interact with the file system, you should be able to determine the size and access nature of the data files that your application will interact with. These files in combination with the security files mak eup a complete Card File Structure (CFS).

In addition, you will need to know whether the smart card needs to perform any encryption operations. The card numbers that end with the letters ED (Encryption) or MC (Math Coprocessor) support encryption mechanisms. Please refer to your selection guide or each card's specification for more information. Encryption features are available within the United States and from those countries that U.S. export restrictions allow. Please contact your CardLogix sales representative for additional information or to request card specifications.

Note: You may change the card type at any time during your file system development.

Pre-Production File System Development Process

The following diagram outlines the M.O.S.T. Card pre-production development process.

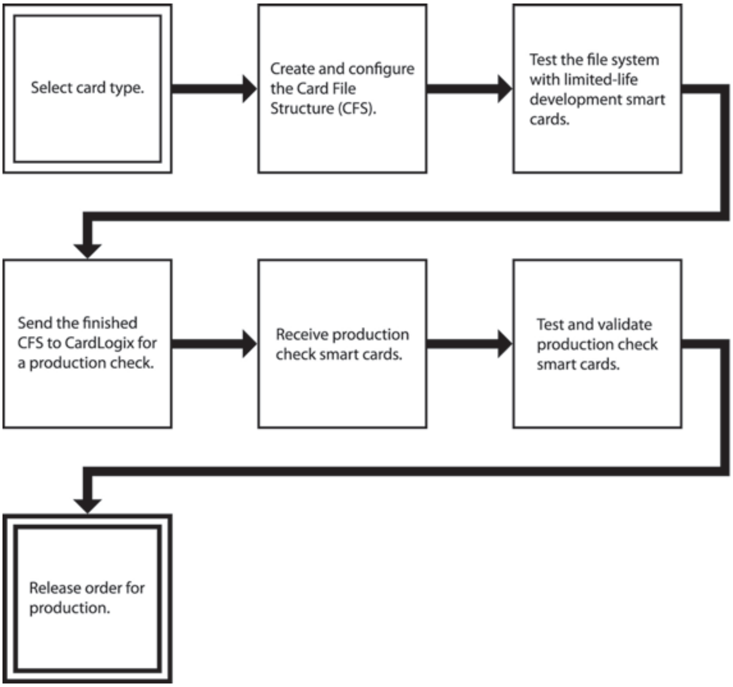

Select card type.
Create and configure the Card File Structure (CFS).
Test the file system with limited-life development smart cards.
Send the finished CFS to CardLogix for a production check.
Receive production check smart cards.
Test and validate production check smart cards.
Release order for production.

Figure 4.1 *- M.O.S.T. Card CFS pre-production development process.*

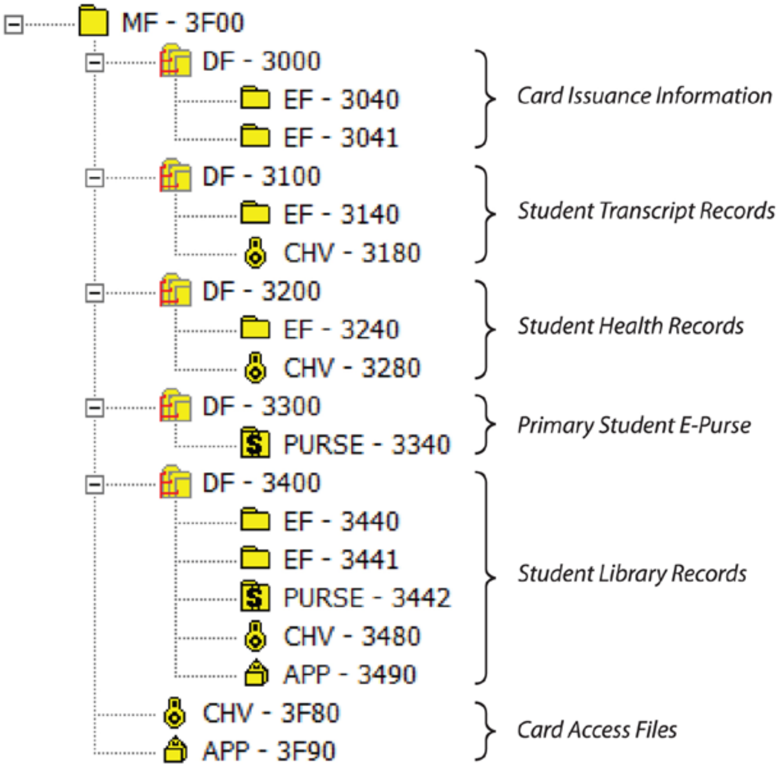
Create and Configure the File System

Using your system application specification as a guide, create the CFS. Refer to section V of this User Guide for more information. When creating a CFS it is best to remember that data tends to fill the entire allotted space.

The ISO 7816-4 format groups application specific files under an umbrella DF. This format has been designed for multi-application functionality and, when executed properly, is the most efficient use of card EEPROM.

The following Example.cfs (which can be found in your Cardfile folder) is a typical layout for separating and establishing separate data layouts by utilizing a DF approach. The Example.cfs demonstrates a fairly simplified layout for a multifunction student ID card for a college environment.

Planning for future functionalities with properly reserved DF groups that can be accessed later by a new application is often a life-saver. Without having to reissue cards an issuer can activate whole new programs that use these reserved DF groups.



Card Issuance Information

Student Transcript Records

Student Health Records

Primary Student E-Purse

Student Library Records

Card Access Files

Figure 4-2: *Example Card File Structure for a Campus ID Card.*

Limited Life Demo Smart Cards with a Test File System

Once your CFS has been created, use the Limited Life smart cards to test the CFS with your application.

> **Note:** If you wish to use the encryption features, please note that the Keys and Hash ID are not programmed into the smart card using M.O.S.T. Toolz. For security purposes, this programming can only be done at CardLogix. Both Limited Life and Fixed File Sample Cards come with the sample keys and Hash ID. Either type of card can be used for testing of encryption. Production check cards will have your specified keys and Hash IDs programmed for complete testing of the application features. For more information please contact your CardLogix sales representative.

Obtain Production Check Smart Cards

To obtain your production check smart cards, please send your CFS file to CardLogix via e-mail or disc. CardLogix will send you three production check smart cards. The production check cmart cards you receive should function exactly to your expectations for production, including all security features. You may lock these files with a password to prevent mistakes or tampering on a production-ready file.

Test and Validate Production Check Smart Cards

Once you have received the three production check smart cards from CardLogix, test them thoroughly with your application. Return one of these three cards to CardLogix with your signature and date noted on the back, along with the Production Configuration Approval Form.

> **Note:** It is your responsibility to ensure that the production check smart cards received are functionally correct and work in your system at the time the production order is released. CardLogix assumes no responsibility for problems that could arise from a change in hardware, software, or system design.

Card Artwork & Personalization

Artwork and volume production printing must be completed before the chips are embedded into the cards. CardLogix has published the "Graphics & Security Printing Guide" to help you prepare for this step. If you need a card designed, the CardLogix in-house agency can provide this service at a very reasonable cost.

Note: The new printing cycle can take **up to 6 weeks** after the artwork is approved and released.

All card personalization such as variable imaging, printing, serialization, database interfacing, mag-stripe encoding, reporting, etc. is described in detail within this guide and should be discussed with your CardLogix sales representative at this time. The best method for receiving exactly what you want, is to provide a specification file or written description of your requirements.

Once you have completed the visual design of your smart card, contact CardLogix at +1 (949) 380-1312, to place your order. Cardlogix will generate a "proof" copy of the card for your approval. Once you approve the card, please return the signed proof and contact your CardLogix sales representative to release the smart cards for final production.

SECTION V: M.O.S.T. TOOLZ™ SOFTWARE OVERVIEW

To use a M.O.S.T. Card®, you must define your file structure, program it into a card, and use an API or low level programming commands to access the card. To define and program the card, CardLogix has developed the M.O.S.T. Toolz™ File Creation Utility. This utility allows you to visually create and save your file structure. It also allows you to program the structure onto a card. To access the card, CardLogix has developed the Winplex® API (Application Programming Interface). The Winplex API contains a series of commands for accessing the card. These commands are implemented as a Microsoft Windows DLL, allowing them to be called from many applications including Microsoft Visual C++, C#, and Visual Basic 6. .NET based compilers such as Visual C# 2008, VB 2008, and C++ 2008 are also able to use Winplex.dll commands.

> *.NET based programs require code marshalling and interop services in order to work with Winplex.dll and the SmartCard services provided by Microsoft. CardLogix provides code samples in C# 2008 and VB 2008 that will demonstrate the required coding.*

Installing the Software

The M.O.S.T. Toolz software is included on a CD-ROM in your toolkit. To install the software:

1. Read and accept the terms of the license agreement
2. Insert the CD-ROM into your CD-ROM drive. If the installation program does not start automatically, run MENU.EXE (located in the root directory of the CD-ROM)
3. Follow the directions on the installation screens

After the installation has successfully completed, the winplex.dll will have been installed in the default directory and a M.O.S.T. Toolz program group will have been added to the programs menu under the CardLogix-CardToolz group.

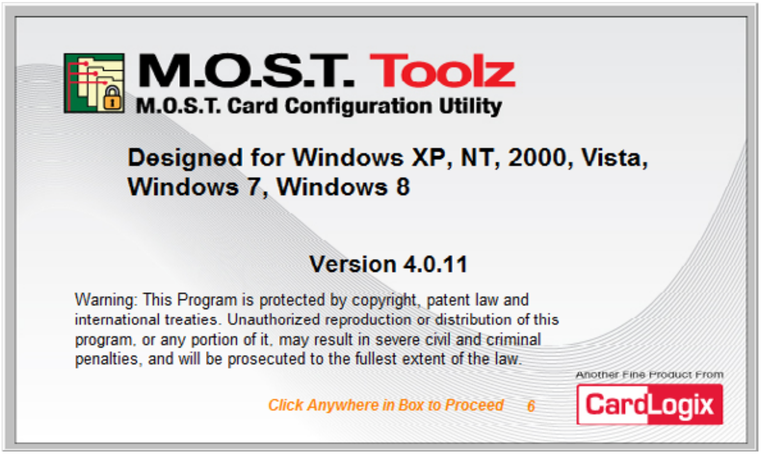
Running the M.O.S.T. Toolz™ File Creation Utility

To run the M.O.S.T. Toolz Card Creation Utility:

4. Open the Start Menu
5. Select Programs
6. Select Smart Toolz (or the program group you specified during the install process)
7. Select M.O.S.T. Toolz™ Card Creation Utility
8. This will launch the M.O.S.T. Toolz Card Creation Utility

Using the M.O.S.T. Toolz™ Card Configuration Utility

The M.O.S.T. Toolz™ Card Configuration Utility allows you to create, save, and program file structures onto your card. When you first launch the program, you will be greeted with a splash screen (Figure 5.1).



M.O.S.T. Toolz
M.O.S.T. Card Configuration Utility

Designed for Windows XP, NT, 2000, Vista, Windows 7, Windows 8

Version 4.0.11

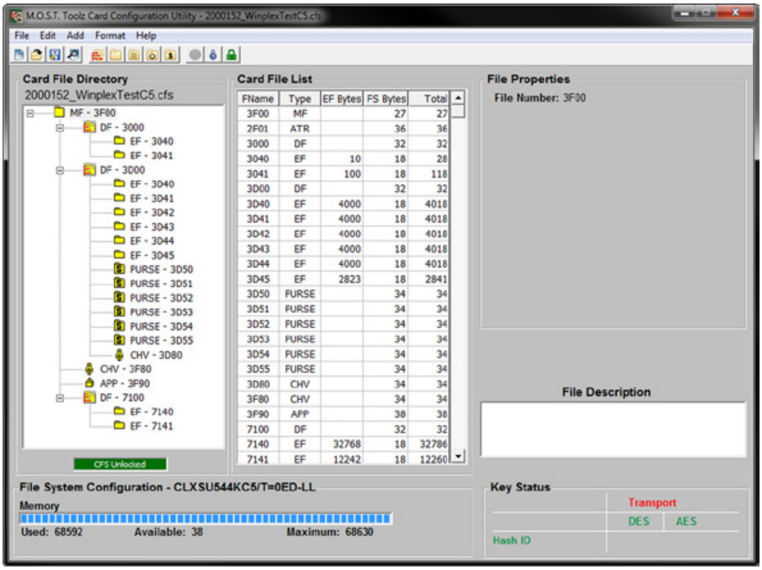
Warning: This Program is protected by copyright, patent law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the fullest extent of the law.

Another Fine Product From CardLogix

Click Anywhere in Box to Proceed 6

Figure 5.1 *- M.O.S.T. Toolz splash screen.*

User your mouse to click anywhere on the splash screen and you will be presented the M.O.S.T. Toolz Card Configuration Utility's home screen (Figure 5.2).



M.O.S.T. Toolz Card Configuration Utility - 2000152_WinplexTestC5.cfs
File
Edit
Add
Format
Help

Card File Directory

2000152_WinplexTestC5.cfs

```
MF - 3F00
    DF - 3000
        EF - 3040
        EF - 3041
    DF - 3D00
        EF - 3D40
        EF - 3D41
        EF - 3D42
        EF - 3D43
        EF - 3D44
        EF - 3D45
        PURSE - 3D50
        PURSE - 3D51
        PURSE - 3D52
        PURSE - 3D53
        PURSE - 3D54
        PURSE - 3D55
        CHV - 3D80
    CHV - 3F80
    APP - 3F90
    DF - 7100
        EF - 7140
        EF - 7141
```

CFS Unlocked

Card File List

FName	Type	EF Bytes	FS Bytes	Total
3F00	MF		27	27
2F01	ATR		36	36
3000	DF		32	32
3040	EF	10	18	28
3041	EF	100	18	118
3D00	DF		32	32
3D40	EF	4000	18	4018
3D41	EF	4000	18	4018
3D42	EF	4000	18	4018
3D43	EF	4000	18	4018
3D44	EF	4000	18	4018
3D45	EF	2823	18	2841
3D50	PURSE		34	34
3D51	PURSE		34	34
3D52	PURSE		34	34
3D53	PURSE		34	34
3D54	PURSE		34	34
3D55	PURSE		34	34
3D80	CHV		34	34
3F80	CHV		34	34
3F90	APP		38	38
7100	DF		32	32
7140	EF	32768	18	32786
7141	EF	12242	18	12260

File Properties

File Number: 3F00

File Description

File System Configuration - CLXSU544KC5/T=0ED-LL

Memory

Used: 68592 Available: 38 Maximum: 68630

Key Status

Figure 5.2 *- M.O.S.T. Toolz home screen.*

The left side will contain a tree view that will hold the list of files you create. The center section shows the files in a list view with information about each file. The program 'remembers' the CFS file name that you worked on previously and will reload that same CFS file the next time you run the program. The right side of the screen will contain the properties for the currently active file. Along the top of the screen is a toolbar that you can use to quickly perform certain functions. These functions include creating or opening a Card File Structure (CFS) file and adding an EF file, CHV file, APP file or Purse File. Along the bottom of the screen you will see a box which indicates how much space is available on the card. This box will fill as you define files on the card.

At startup, the card file directory will show your most recently opened CFS file. If you would like to open a different file system, or if you wish to use one of the examples, you can click on the Open icon in the toolbar to open the selection dialog box.

To add a file to the CFS, click on the corresponding icon in the toolbar or select the file type from the Add menu. The type of item you may add depends on the currently selected file. If you have selected the MF, you may add any type of file. If you have selected a DF, you may add any type of file except for another DF. If you have selected a CHV, APP, EF, or Purse, you may not add any other file types. You should keep in mind that file structures are organized using a tree type structure that represents the relational requirements of the different files. This tree structure enforces a parent-child relationship for files. Since CHVs, APPs, EFs, and Purses are files, they cannot have any children. The program prevents you from creating children for these types of files. A DF is a directory and can have children, however, DFs are not allowed to have other DFs as children. The MF is the unique master file. It is the root of the tree and can have any other type of file as a child.

Using idblox® files with M.O.S.T. Toolz

The idblox® credential ecosystem provides a streamlined solution for high security ID card development, deployment, and use. By using components from idblox vendors, you can build your system without all of the problems that typically result from data incompatibilities between different applications. The idblox CFSs included in this version of M.O.S.T. Toolz are but a few of a growing list of Logical Data Structures (LDSs) that can save vendors from having to program a new software application every time. Please check with your CardLogix Sales Representative for the most current list.

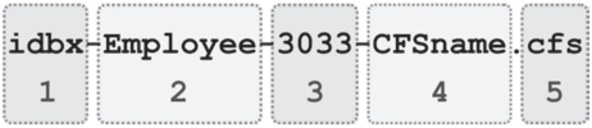
The only thing needed is the secure distribution of keys and activation by that application vendor. This also saves the vendor the trouble of programming a solution themselves. idblox has many pre-configured LDSs in .cfs templates—all configuration is already done for you! The only thing the designer or issuer has to do is create and distribute keys.

For true data interoperability, each element must be consistent in its size, encoding method, and storage location. This can be accomplished by using the provided templates (`IDBX-xxxx-xxxx-xxxxx.cfs` files). This consistency allows all idblox vendors to build their applications under one unified data model and simply change keys for each customer implementation. Unlike the data architecture in PIV or ICAO passport cards, the idblox data architecture has segmented the data elements for true multiple-application access. idblox utilizes common data elements from ICAO, NIST, EMV, and the EU driver's license standards.

Regardless of the idblox card's data model, either you or the card issuer (key maker) must make or assign keys for the CFS:

1. Use the pull-down menus in M.O.S.T. Toolz to generate keys. Start with all the keys listed under `Edit` in the program menu. Fill in each of these keys with your values or press the `Random` button to have the values automatically generated for you. Press the `Save` button when you are done.
2. If you want to use a Global Password to protect the entire card, enter a password in the ASCII or hexadecimal textboxes using the appropriate values. Press the `OK` button when you are done.
3. Each CHV and APP file in the Card File List will need to be modified with your keys to protect each pre-designated EF or Purse File. Simply enter a password in ASCII or enter hexadecimal values in the provided textboxes. Press the `OK` button when you are done.
4. Save your CFS as a new file by choosing `File > Save As...` in the application menu. In order to guarantee compatibility with idblox tools, you must use the following filename format for your .cfs file (Figure 5.3).

idbx-Employee-3033-CFSname.cfs



```
1. idblox file template ID & lock (locked)
2. General description and use case (locked)
3. Next number in series (locked)
4. Unique CFS identifier (chosen by the customer)
5. Card File Structure extension (locked)
```

***Figure 5.3** – idblox CFS filename format example.*

5. The keys now need to be saved to an external file outside of M.O.S.T. Toolz. This is done by selecting `File > Export to CSV` in the program menu. The resulting .csv file can be read by Microsoft Excel and many other programs. A formatted sample of a .csv file is included for reference in the `C:\Program Files (x86)\CardLogix Card Toolz\Documentation` directory.
6. Lock the .cfs file with a simple password. This is done by selecting `File > Lock CFS file` in program menu. M.O.S.T. Toolz should save this change automatically.

Once this procedure is complete, you may distribute each specific key group to your chosen idblox third-party vendor for system activation and use. This secure exchange is called a "Key Ceremony". Typically, vendors will deliver keys through e-mail with PGP encryption for security.

Note that when a credential is to be issued, the issuer must upload the Card File Structure (.cfs file), Card Project File (.cpf file), or applet into CardLogix' Card Encoding Engine application for auto-population of the collected data into the chip. Programming is not required.

Creating a Custom Card File Structure

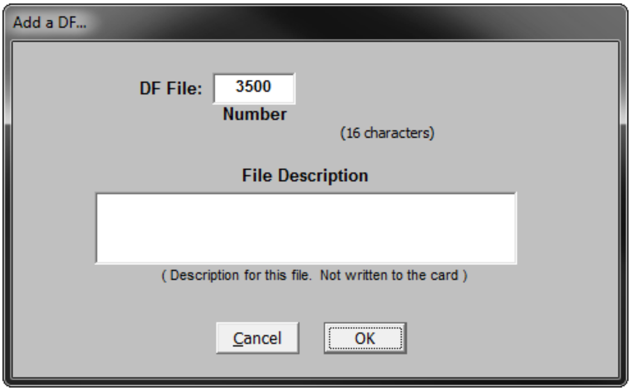
Before creating your file system, you should first create a file system on paper. This is typically done as part of a system document that outlines all card, hardware, and software interactions. This will allow you to easily translate your design to an actual file system. Select `File > Open` from the main menu. Enter a name for your custom file system and save it. Select a card type from the new menu. To add a file to the system, click on the appropriate file type icon in the toolbar or select the file type from the `Add` menu. The items in this menu can only be selected if they can be added under the currently selected item. For example, if you have a DF selected, you will be able to add an EF, Purse, CHV, or APP. However, if you have an EF selected, you will not be able to add any items.

Setting the File Properties

Each file has a different set of properties associated with it. This section explains the properties for each type of file.

DF Files

When you click on the Add DF icon or select Add DF from the Add menu, the "Add a DF..." dialog box appears (Figure 5.4). You can use this dialog box to change the name of the DF. A valid, default name for the DF is automatically generated by the program. If you change the name of the DF, it will be verified for correctness when you click on the OK button. If the DF name you select is invalid or already exists, an appropriate error message will be generated. To create the new DF, click on the OK button. To exit this dialog box without saving the DF, click on the Cancel button.



Add a DF...

DF File: 3500
Number
(16 characters)

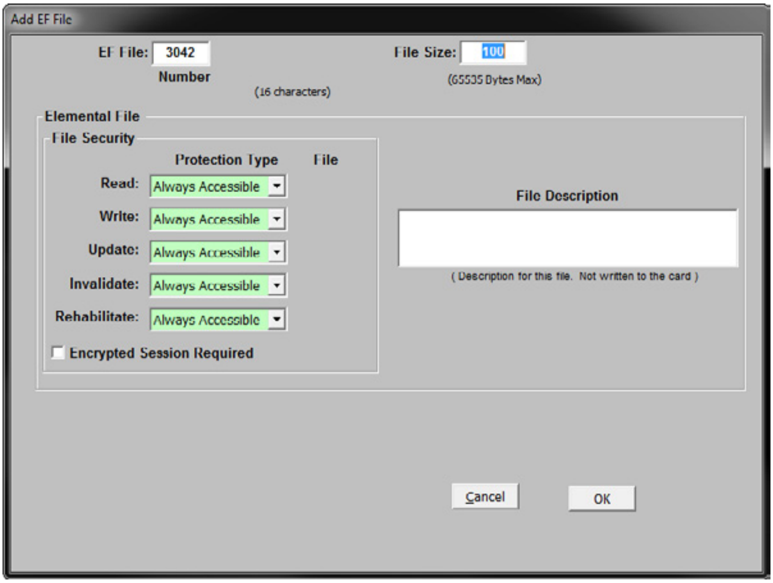
File Description

(Description for this file. Not written to the card)

Figure 5.4 - `Add a DF...` *dialog box.*

Transparent Files

When you click on the Add EF icon or select Add EF from the Add menu, the "Add EF File" dialog box appears.



Add EF File

EF File: 3042
Number
(16 characters)

File Size: 100
(65535 Bytes Max)

Elemental File

File Security

	Protection Type	File
Read:	Always Accessible	
Write:	Always Accessible	
Update:	Always Accessible	
Invalidate:	Always Accessible	
Rehabilitate:	Always Accessible	

□ Encrypted Session Required

File Description

(Description for this file. Not written to the card)

Figure 5.5 - `Add EF File` *dialog box.*

To edit an existing EF, you can double-click on the desired EF in the list or tree. You can use the dialog box that appears to change the properties of the EF. If you have selected Add EF, the EF name will be automatically generated by the program. You may change this name. However, the program must verify that the name is correct before it will close the dialog box. If the name you have selected is invalid, an error message will be displayed.

Using this dialog box, you can also specify the different protections on the file. As explained in Section 4, an EF can have four types of protection: Always Accessible, Never Accessible, CHV Protected, and APP Protected. If you select Always Accessible for an access type, that feature of the EF is always available. If you select Never Accessible, that feature of the EF is never available (and will not work). If you select CHV Protected, that feature of the EF is only available after the CHV password has been verified. You may specify a CHV that is either associated with the current DF or the MF. Any other CHV is not allowed. If you select APP Protected, that feature of the EF is only available after the APP has been authenticated. You may specify a CHV that is either associated with the current DF or the MF. If you specify an invalid CHV or APP name, the program will generate an error message.

If you specify CHV Protection or APP Protection, a box will appear where you must enter the filename of the CHV or APP you want the feature protected by. The protection file must already exist in the CFS and can be defined in either the current DF or the MF.

You should use the File Size field to specify the size of the file on the card in bytes. The size of the file is only limited by the size of the data area on the card.

If you want the file's data to be encrypted when it is being transmitted to or from the card, you need to check the Encrypt File checkbox. This marks the file as a secure file that can only be accessed using the Winplex© API secure commands (or directly using the secure APDUs commands described in your M.O.S.T. Card® specification). This only works on cards with part numbers ending in ED or MC. Please note that this selection turns on transmission encryption only and pertains to the transmission and reception of data to the card. This encryption method is designed to prevent interception of readable data by sniffing devices that monitor the reader wires. After turning on the encryption selection, reads and writes to this file will require either AES, DES or 3DES encrypt and decrypt. Received data can be decrypted with AES, DES or 3DES regardless of the encryption method used in saving data. If you want your data to be stored in encrypted form on the card you must encrypt the data with your own encoding function before sending the data to the file.

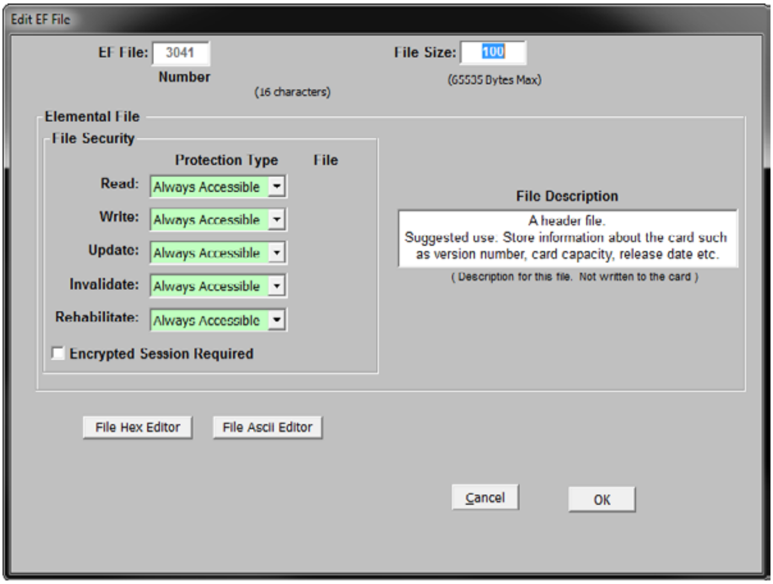
Data that is already encrypted may not need to be transmitted using encryption.

An optional file description box allows you to type in any description of your choosing for this file. The description information that you type into this box is not written to the card itself, it is only saved to the CFS file. This description is strictly for your convenience in helping you to remember the purpose of each file.

To save your changes, click on the OK button. Your settings for the EF will be verified and stored. If any values are incorrect, an error will be displayed. To exit the dialog box without saving your changes, click on the Cancel button.

The Transparent File Editor

Below the EF file dialog, a file editor is available to allow for simple editing of EF file contents. This feature allows you to make simple edits of the contents of an EF file on a card written with the tool. This is only for testing and debugging purposes only and and data entered and saved into an EF file will not be saved as part of your CFS file. To turn on the EF file editor, click on the Edit Mode dialog box (Figure 5.6).



Edit EF File

EF File: 3041
Number
(16 characters)

File Size: 100
(65535 Bytes Max)

Elemental File

File Security

	Protection Type	File
Read:	Always Accessible	
Write:	Always Accessible	
Update:	Always Accessible	
Invalidate:	Always Accessible	
Rehabilitate:	Always Accessible	

□ Encrypted Session Required

File Description

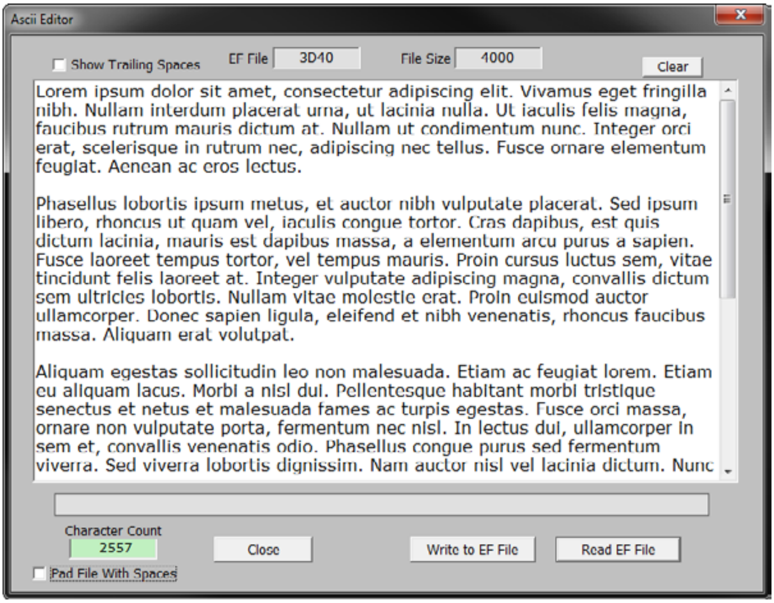
A header file.
Suggested use. Store information about the card such as version number, card capacity, release date etc.

(Description for this file. Not written to the card)

Figure 5.6 - `Edit EF File` *dialog box.*

Before an EF file can be edited, the card file structure (CFS) must have already been written to the card. After entering the edit mode, the CFS will be compared against the card to make sure that it matches. When the file compare dialog box comes up, click OK to allow the CFS to be compared to the card content. If the CFS matches what the data on the card, the editor features will be enabled.

Once editing features are enabled, you may edit the EF file content in either Hex or ASCII mode. In ASCII mode, only those characters that are normally visible in standard text documents will be shown while other characters (such as hex FF) will not. Data to be entered can be typed in one character at a time in either hex or ASCII mode, or data can be loaded into the clipboard and pasted into the editor. Clipboard data can be loaded by selecting a file to copy from or by copying data into the clipboard from another application. After editing is completed, you may either click OK to write the data to the EF file or click close to discard the data without writing it. Data in the editor will be truncated to the maximum size of the EF file.



□ Show Trailing Spaces

EF File 3D40

File Size 4000

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus eget fringilla nibh. Nullam interdum placerat urna, ut lacinia nulla. Ut iaculis felis magna, faucibus rutrum mauris dictum at. Nullam ut condimentum nunc. Integer orci erat, scelerisque in rutrum nec, adipiscing nec tellus. Fusce ornare elementum feugiat. Aenean ac eros lectus.

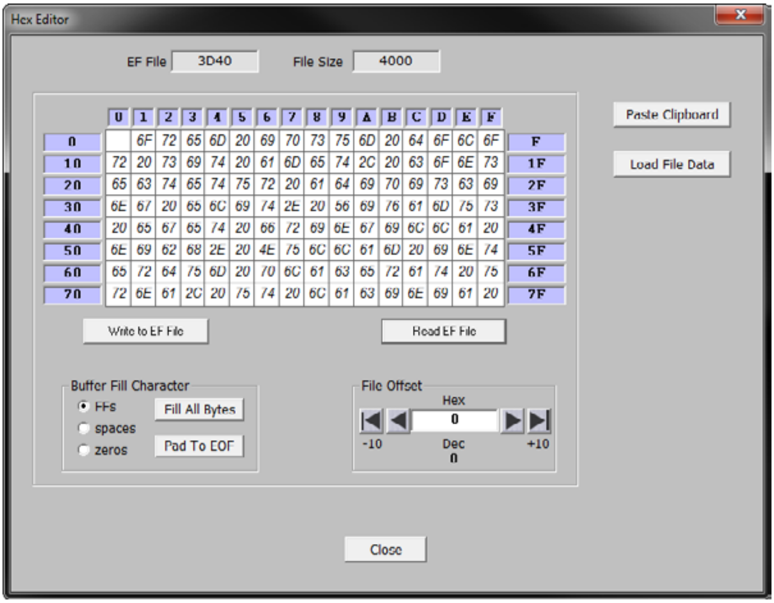
Phasellus lobortis ipsum metus, et auctor nibh vulputate placerat. Sed ipsum libero, rhoncus ut quam vel, iaculis congue tortor. Cras dapibus, est quis dictum lacinia, mauris est dapibus massa, a elementum arcu purus a sapien. Fusce laoreet tempus tortor, vel tempus mauris. Proin cursus luctus sem, vitae tincidunt felis laoreet at. Integer vulputate adipiscing magna, convallis dictum sem ultricies lobortis. Nullam vitae molestie erat. Proin euismod auctor ullamcorper. Donec sapien ligula, eleifend et nibh venenatis, rhoncus faucibus massa. Aliquam erat volutpat.

Aliquam egestas sollicitudin leo non malesuada. Etiam ac feugiat lorem. Etiam eu aliquam lacus. Morbi a nisl dui. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Fusce orci massa, ornare non vulputate porta, fermentum nec nisl. In lectus dui, ullamcorper in sem et, convallis venenatis odio. Phasellus congue purus sed fermentum viverra. Sed viverra lobortis dignissim. Nam auctor nisl vel lacinia dictum. Nunc

Character Count 2557

□ Pad File With Spaces

Figure 5.7 - *`ASCII Editor` dialog box.*



EF File 3D40

File Size 4000

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0		6F	72	65	6D	20	69	70	73	75	6D	20	64	6F	6C	6F	F
10	72	20	73	69	74	20	61	6D	65	74	2C	20	63	6F	6E	73	1F
20	65	63	74	65	74	75	72	20	61	64	69	70	69	73	63	69	2F
30	6E	67	20	65	6C	69	74	2E	20	56	69	76	61	6D	75	73	3F
40	20	65	67	65	74	20	66	72	69	6E	67	69	6C	6C	61	20	4F
50	6E	69	62	68	2E	20	4E	75	6C	6C	61	6D	20	69	6E	74	5F
60	65	72	64	75	6D	20	70	6C	61	63	65	72	61	74	20	75	6F
70	72	6E	61	2C	20	75	74	20	6C	61	63	69	6E	69	61	20	7F

Buffer Fill Character
● FFs
○ spaces
○ zeros

File Offset
Hex 0
-10 +10
Dec 0

Figure 5.8 - *`Hex Editor` dialog box.*

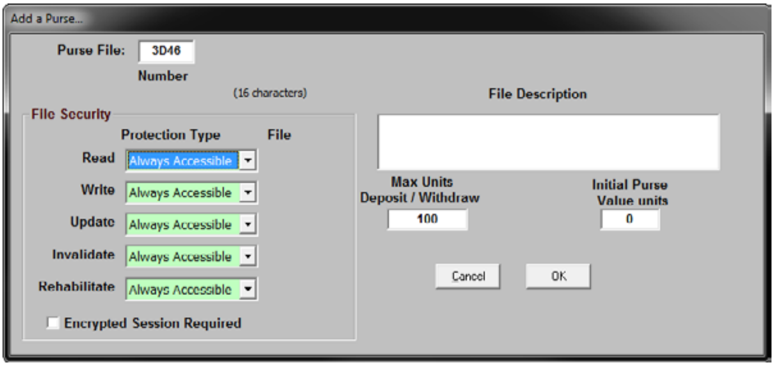
Please note that making changes to the EF file's size, security protections, file name, etc. will require you to write the EF file changes to the card before you can write any data to the EF file. Therefore, any such changes that occur while in the EF file edit mode will disable the edit mode feature.

Write Fill Character

Whenever you use the EF file editor, if the data you are writing contains fewer characters than the size of the file, the remaining bytes can be optionally filled in with hex value 00, FF or 20. If this feature is turned off, the existing byte values in the card will not be altered. The value for an erased file byte in a new card will be FF.

Purse Files

When you click on the Add Purse icon or select Add Purse from the Add menu, the "Add a Purse..." dialog box opens (Figure 5.9). To edit an existing Purse, you can double-click on the desired Purse in the list or tree.



Purse File: 3D46
Number
(16 characters)
File Description
Protection Type File
Read: Always Accessible
Write: Always Accessible
Update: Always Accessible
Invalidate: Always Accessible
Rehabilitate: Always Accessible
□ Encrypted Session Required
Max Units Deposit / Withdraw: 100
Initial Purse Value units: 0

Figure 5.9 *-* `Add a Purse...` *dialog box.*

You can use this dialog box to change the properties of the Purse. If you have selected Add Purse, a default Purse name will automatically be generated by the program. You may change this name. However, the program must verify that the name is correct before it will close the dialog box. If the name you have selected is invalid, an error message will be displayed.

Using this dialog box, you can also specify the different protections on the file. As explained in Section 4, a Purse can have four types of protection: Always Accessible, Never Accessible, CHV Protected, and APP Protected. If you select Always Accessible for an access type, that feature of the Purse is always available. If you select Never Accessible, that feature of the Purse is never available (and will not work). If you select CHV Protected, that feature of the Purse is only available after the CHV password has been verified. You may specify a CHV that is either associated with the current DF or the MF. Any other CHV is not allowed. If you select APP Protected, that feature of the Purse is only available after the APP has been authenticated. You may specify a CHV that is either associated with the current DF or the MF. If you specify an invalid CHV or APP name, the program will generate an error message.

If you specify CHV Protected or APP Protected, a dialog box will appear where you must select the filename of the CHV or APP that you want to protect the feature with. The protection file must already exist and can be defined in either the current DF or the MF.

You must specify a maximum withdrawal value for the purse in the Maximum Withdrawal Value field. You may optionally enter an initial purse value or you may leave the default value of 0 (meaning no limit).

An optional file description can be entered into the File Description text box. This description is saved to your CFS file but is not written to the card itself. This description information is only for your convenience in helping you to remember the purpose for each file.

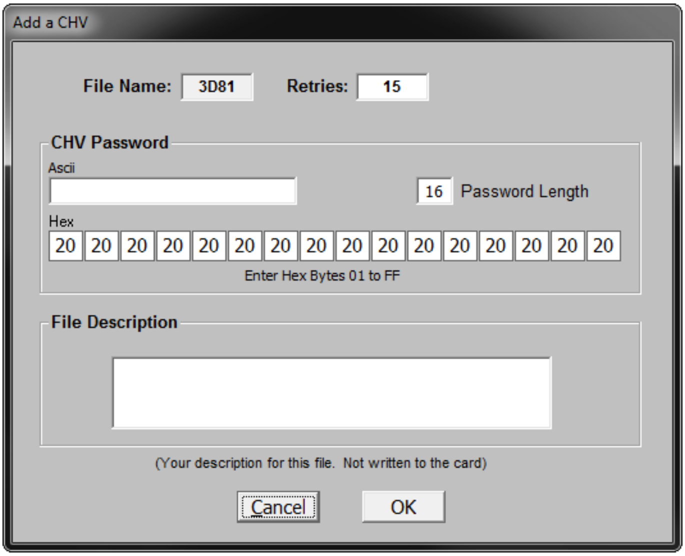
We recommend that the file's data be encrypted when it is being transmitted to or from the card, you need to check the Encrypted Session Required checkbox. This marks the file as a secure file that can only be accessed using the Winplex API secure commands (or directly using the secure APDUs commands described in your M.O.S.T. Card specification). This only works on cards with part numbers ending in ED. Please note that this selection turns on transmission encryption only and pertains to the transmission and reception of data to the card. Data is not stored on the card in encrypted form. This encryption method is designed to prevent interception of readable data by sniffing devices that monitor the reader wires. After turning on the encryption selection, reads and writes to this file will require either AES, DES or 3DES encrypt and decrypt. Received data can be decrypted with AES, DES or 3DES regardless of the encryption method used in saving the data. If you want your data to be stored in encrypted form on the card you must encrypt the data with your own encoding function before sending the data to the file.

To save your changes, click on the OK button. Your settings for the Purse will be verified and stored. If any values are incorrect, an error will be displayed. To exit the dialog box without saving your changes, click on the Cancel button.

Linear and cyclic EFs are designed for structured record keeping functions with a purse file, such as transactions. Each file type behaves in a similar fashion but with the cyclic file, after the preset number of records is reached, the write function will overwrite the oldest record. The access functions are detailed in the specifications.

CHV Files

When you click on the Add CHV icon or select Add CHV from the Add menu, the "Add a CHV..." appears (Figure 5.10). To edit an existing CHV, you can double-click on the desired CHV in the list or tree.


Add a CHV

File Name: 3D81 Retries: 15

CHV Password

Ascii

16 Password Length

Hex

20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Enter Hex Bytes 01 to FF

File Description

(Your description for this file. Not written to the card)

Figure 5.10 - `Add a CHV` *dialog box*

You can use this dialog box to change the properties of the CHV. If you have selected Add CHV, a CHV name will be automatically generated by the program. You may change this name. However, the program must verify that the name is correct before it will close the dialog box. If the name you have selected is invalid, an error message will be displayed.

You may also use this dialog box to set the password for the CHV. The CHV password can be from 4 to 16 characters in width. It may contain any ASCII or Hex character you care to enter.

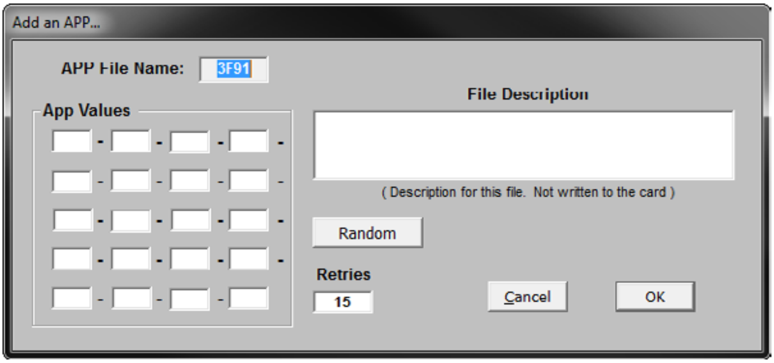
You should use the Retries field to specify the number of retries allowed for the CHV. The number of retries defines the number of incorrect CHV verifications that can be presented before the CHV is locked out and rendered inaccessible. The number of retries ranges from 1 to 15. Each incorrect CHV verification decreases the retry counter by one. When the counter reaches 0, the CHV is no longer valid and all further attempts to validate the CHV will fail. A successful verification of the CHV will reset the retry counter if it has not yet been invalidated.

An optional file description can be entered into the File Description text box. This description is saved to your CFS file but is not written to the card itself. The description information is only for your convenience to help you remember the purpose of the file.

To save your changes, click on the OK button. Your settings for the CHV will be verified and stored. If any values are incorrect, an error message will be displayed. To exit the dialog box without saving your changes, click on the Cancel button.

APP Files

When you click on the Add APP icon or select Add APP from the Add menu, the "Add an App..." dialog box appears.

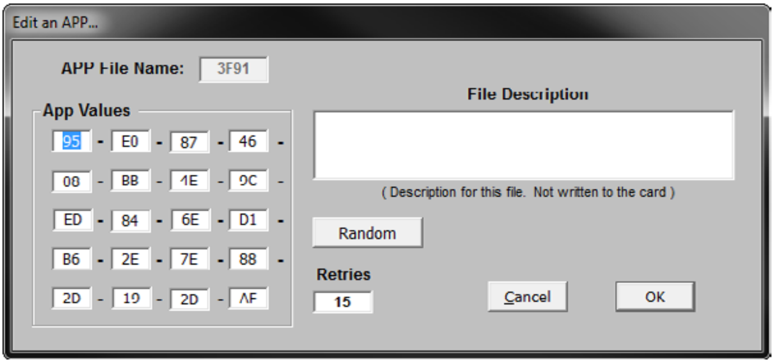

Add an APP...

APP File Name: 3F91

Retries: 15

Figure 5.11 - `Add an APP...` *dialog box.*

To edit an existing APP, you can double-click on the desired APP in the list or tree.


Edit an APP...

APP File Name: 3F91

App Values:
95 - E0 - 87 - 46 -
08 - BB - 4E - 9C -
ED - 84 - 6E - D1 -
B6 - 2E - 7E - 88 -
2D - 19 - 2D - AF

Retries: 15

Figure 5.12 - `Edit an APP...` *dialog box.*

Each of the CardLogix M.O.S.T. card families handle APPs slightly differently. The following table outlines these differences.

Table 5.1 - M.O.S.T. Card APP File differences.

Card Family	Status	APP Authentiction	APP Token
K-Series (M.O.S.T. -lc)	Deprecated	Proprietary	8 bytes
CO-Series	Deprecated	DES	8 bytes
F-Series	Deprecated	None	None
J-Series	Deprecated	SHA-1	20 bytes
C-Series	Active	SHA-1, SHA-2	20 bytes, 40 bytes

You may also use this dialog box to set the authentication code for the APP. The APP authentication code must be 20 bytes long. The APP Value fields represent a 20 byte authentication value. Each field holds one hexadecimal byte. This allows each field to range from 00 to FF (0 to 255 decimal).

You should use the Retries field to specify the number of retries allowed for the APP. The number of retries defines the number of incorrect APP authentications that can be presented before the APP is locked out and rendered inaccessible. The number of retries can range from 1 to 15. Each incorrect APP authentication decreases the retry counter by one. When the counter reaches 0, the APP is no longer valid and all further attempts to validate it will fail. A successful authentication of the APP will reset the retry counter. An optional file description can be entered into the File Description text box. The description is saved to your CFS file but is not written to the card itself. This description information is only for your convenience to help you remember the purpose of the file.

To save your changes, click on the OK button. Your settings for the APP will be verified and stored. If any values are incorrect, an error will be displayed. To exit the dialog box without saving your changes, click on the Cancel button.

Writing to a Limited Life Card

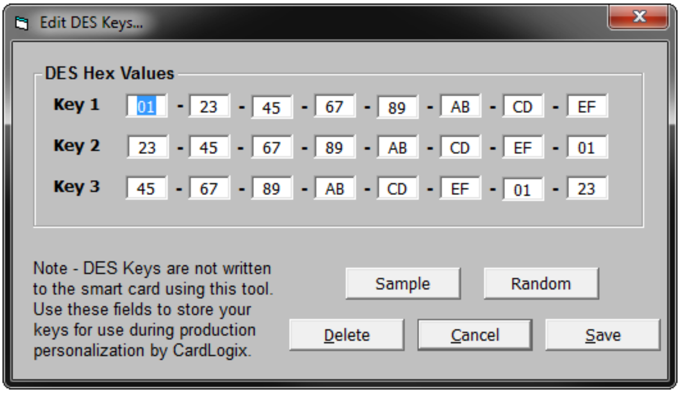
Once you have defined your file system, you need to program it into a card. To write to a card, follow these steps:

7. Save your file.
8. Select File -> Reader Setup to verify you have selected the correct reader.
9. Select File -> Card Setup to verify the card type you will be programming.
10. Select Format -> Write to Card

DES Keys

Some cards come with DES encryption capabilities. When you select DES Keys from the menu, the "Edit DES Keys..." dialog box appears (Figure 5-12). Enter your DES key data into all of the fields in hexadecimal format. These values will be used in generating session keys and should be guarded carefully.

> ***Note:*** All keys are saved to your CFS file for later use in creating your production cards, and are not written to your sample card. Sample cards will continue to contain sample card keys that you may use for testing purposes.



DES Hex Values

Key 1 01 - 23 - 45 - 67 - 89 - AB - CD - EF

Key 2 23 - 45 - 67 - 89 - AB - CD - EF - 01

Key 3 45 - 67 - 89 - AB - CD - EF - 01 - 23

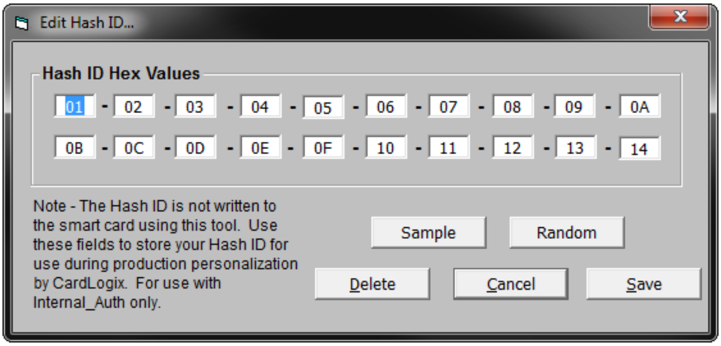
Note - DES Keys are not written to the smart card using this tool. Use these fields to store your keys for use during production personalization by CardLogix.

Figure 5.13 - `Edit DES Keys...` *dialog box.*

HASH IDs

All M.O.S.T. cards come with authentication capabilities. When you select Hash ID from the Edit menu, the dialog box appears (Figure 5-13). Enter your Hash ID key data into all of the fields in hexadecimal values.

> ***Note:*** The Hash ID is not saved to the card. Sample cards have an unchangeable sample Hash ID in them that can be used for testing.



Hash ID Hex Values

01 - 02 - 03 - 04 - 05 - 06 - 07 - 08 - 09 - 0A

0B - 0C - 0D - 0E - 0F - 10 - 11 - 12 - 13 - 14

Note - The Hash ID is not written to the smart card using this tool. Use these fields to store your Hash ID for use during production personalization by CardLogix. For use with Internal_Auth only.

Figure 5.14 - `Edit Hash ID...` *dialog box.*

Viewing Information About the Current Card

This important data can be retrieved in the M.O.S.T. Toolz File Creation utility by choosing `Help > Current Card Info (Ctrl +Z)` from the program menu.

Your card management and issuance software should handle the distribution and management of each card's Transport Keys. Viewing card information from your application provides ancillary information that can be helpful in determining if the card has been tampered with or if there are problems with changing card state between active and inactivate.

Retrieving the card's forensic data can also be accessed by using the Winplex command `CLX_GetPublicInfo`.

This feature displays the following information:

- Card family
- OS version (short)
- OS version (long)
- CardLogix serial number (GUID)
- OS Lock Byte status
- Password counters (for both the master access password and user access passwords)
- Maximum file space
- Available file space
- Chip serial number
- Limited-life counter
- Incorrect file select counter
- Bad transport key counter

M.O.S.T. Toolz Program Menu Command Summary

Table 5.2 - File Menu Commands

Command	Function
New	Create a new file structure. The current file structure will be closed and a new empty file structure will be created.
Open	Open an existing file structure. The current file structure will be closed and the selected file structure will be opened.
Close	Close the current file structure.
Save As	Save the current file structure under a different name.
Export to CSV	Export the file structure to a text-based file that contains all parameters surrounding your card, including keys. A locked file cannot be exported.
Reader Setup	Configure M.O.S.T. Toolz to use a specific reader by choosing `Find USB Readers`, selecting the reader you want to use from the list of connected readers, pressing the `Set Reader` button, and finally pressing the `OK` button.
Card Setup	Specify the type of card that you are using. In the dialog box that appears, select the appropriate card type and then pressing the `OK` button.
Lock CFS File	Lock your CFS file using a 4 character password. This helps to prevent unauthorized or unintentional changes to your CFS file. Some of the supplied sample CFS files will be locked using the password `1234`. You may unlock these files to change them, but it is recommended that you work with copies of these files, keeping the original ones intact. If you attempt to make changes to a CFS file that has been locked, the red "CFS Locked" indicator will flash. When sending your finished CFS file to CardLogix, please provide your password. In most cases, CardLogix will not need to unlock the CFS file. NOTE: Locking your CFS file will not prevent tampering of the file using external editing tools, it is only intended to help protect against inadvertent changes while using M.O.S.T. Toolz.
Unlock CFS File	Unlock the CFS file with a 4-character password to allow changes to the file.
Remember Last CFS	Configure M.O.S.T. Toolz to remember the most recently opened file.
Exit	Close and exit the program.

Table 5.3 - Edit Menu Commands

Command	Function
Edit	Modify the currently selected DF, EF, CHV, APP, or Purse File.
Delete File	Delete the currently selected file. If the file is a DF, you will be prompted to verify the deletion.
AES Keys	Enter your AES Keys.
DES Keys	Enter your DES Keys.
HASH ID	Enter your HASH IDs.
HMAC Keys	Enter your HMAC Keys.
Administrator Keys	Enter your Administrator Keys.
Transport Keys	Enter your Transport Keys.

Table 5.4 - Add Menu Commands

Command	Function
Add Global Password	Add password protection to the file structure. When you select this command, the "Add a Global Password..." dialog box will appear. Enter the password and then press the `OK` button to save the new GPF.
Add DF	Add a new DF to the file structure. When you select this command, the "Add a DF..." dialog box will appear. Press the `OK` button to save the new DF.
Add Transparent EF	Add a new EF to the file structure. Transparent EFs are used for data storage. When you use this command, the "Add EF File" dialog box will appear. Press the `OK` button to save the new EF.
Add Cyclical EF	Add a new Cyclical EF to the file structure. Cyclic EFs are used for record-based transactions. When you use this command, the "Add Cyclic File" dialog box will appear. Press the `OK` button to save the new Cyclic EF.
Add Linear EF	Add a new Linear EF to the file structure. Linear EFs are for record-based transactions. When you use this command, the "Add Linear File" dialog box will appear. Press the `OK` button to save the new Linear EF.
Add Purse	Add a new Purse File to the file structure. When you select this command, the "Add a Purse" dialog box will appear. Press the `OK` button to save the new Purse File.
Add CHV	Add a new CHV to the file structure. When you select this command, the "Add a CHV" dialog box will appear. Press the `OK` button to save the new CHV.
Add APP	Add a new APP to the file structure. When you select this command, the "Add an APP" dialog box will appear. Press the `OK` button to save the new APP.

Table 5.5 - Format Menu Commands

Command	Function
Lock File System	Use this command to lock the file system that you are programming onto a card. If you lock the file structure on a card, it cannot be changed. When Lock File System is enabled, this menu item will have a checkmark.
Write to card	Use this command to write the current file structure to a card. When you select this command, a dialog box will appear showing the status of the writing. When the writing has completed, the dialog box will automatically close.
Verify File System	Use this command to confirm the CFS on the card matches the CFS that is currently open in the M.O.S.T. Toolz Card Configuration Utility.
Get ATR	This command repowers the card and retrieves the Answer to Reset data string.

Table 5.6 - Help Menu Commands

Command	Function
Current Card Info	Display ancillary data about the card that is currently inserted in the card reader or terminal.
Contents	Display a list of the various help topics.
Search for Help on	Search for help on a particular topic.
About M.O.S.T.™ Toolz	Display software information about the M.O.S.T. Toolz Card Configuration Utility.

SECTION VI: ACCESSING THE CARD WITHOUT USING WINPLEX®

The Winplex® API is not practical for all environments. The API is designed to work with systems that run a Microsoft Windows operating system. If your card is being deployed into a non-Windows environment, you will need to access the card using low-level APDU commands. These commands follow the ISO 7816 specification. The actual commands supported are card-specific. For more information on the structure of the commands, you should reference the M.O.S.T. Card® specification for the card that you are using. The M.O.S.T. Card specification details the format of each command. You should keep in mind that the reader you use to communicate with the card might have its own command structure that encapsulates the APDU command that you are sending. In this case, you would need to obtain an API for that reader to communicate with the card.

Microsoft PC/SC API

In the Windows environment, you also have a choice about which API to use. The Winplex API is designed to support all features of a CardLogix card and many non-smart card features that the smart card readers support such as host-based encryption, mag-stripe functionality, LED control and card transport management. However, the Winplex API only supports a limited number of card readers. Microsoft sponsored the development of the PC/SC API for communicating with smart cards and readers. To use this API, you must have appropriate drivers for both the smart card and the reader that you are using. For more information on using this API, you should consult the Microsoft website or platform SDK.

Microsoft supports the Personal Computer/Smart Card (PC/SC) interface to smart cards and readers. In this environment, every smart card has its own Smart Card Service Provider (SCSP) and an optional Cryptographic Service Provider (CSP). Microsoft publishes a list on their website of the various smart card readers that have been certified to work with this API. CardLogix has many of these readers available for sale at www.cardlogix.com.

APPENDIX A: SYSTEM DEPLOYMENT RECOMMENDATIONS

1. Establish clear and achievable program objectives
2. Analyze the application and IT enviroment
3. Make sure that the organization has a stake in the project's success and that management buys into the program
4. Set a budget
5. Name a project manager
6. Assemble a project team and create a team vision
7. Graphically create a dataflow diagram
8. Assess the card and reader options
9. Write a detailed specification for the cards and system
10. Set a realistic schedule with inchstones and milestones
11. Establish security parameters for people and the system
12. Build your on-card and host file systems
13. Phase in each system element and test as you deploy
14. Reassess your system for security leaks
15. Deploy the first phase of cards and test the system
16. Train the key employees responsible for each area
17. Set up a system user manual
18. Check the reporting structures
19. Create contingency plans
20. Deploy and announce your system
21. Advertise and market your system

APPENDIX B: PROGRAMMING NOTES

To assist you with the special programming requirements for working with Smart Cards, we have included source code examples in several high level programming languages on the M.O.S.T. Toolz disc.

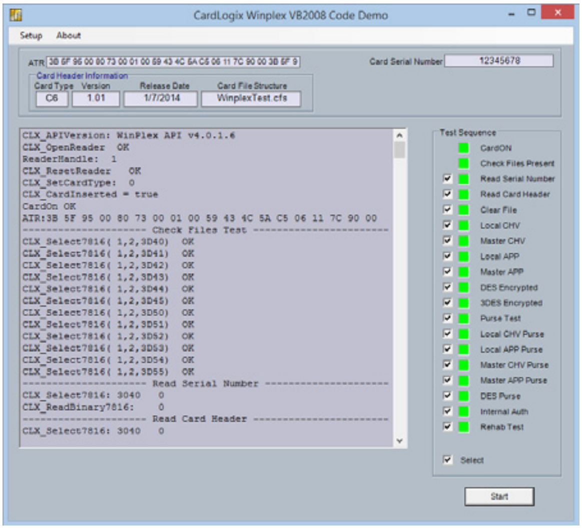
The programming examples included with Winplex are designed to work with a special CFS file that is included with M.O.S.T. Toolz called WinplexTest.cfs. That CFS includes files that are useful in demonstrating most of the possible ways to interact with card files using our Winplex API.

To use the programming examples, open WinplexTest.cfs with the M.O.S.T. Toolz Card Configuration Utility and write that CFS file to one of your limited-life sample cards. Once written to the card, use the Verify File System command from the Format menu to confirm that the CFS was written to the card correctly.

With the CFS file successfully written to the card, chose and open one of the programming examples provided in the Winplex TestApps folder for the programming language of your choice. We have included examples for Visual C++ 6, Visual Basic 6, Visual C# 2008 and Visual Basic 2008.

You will be able to run the program or step through the source code to observe the steps required for the card functions that you want to use. You may disable any function that you do not want to include.

CardLogix will be glad to help you with questions that you may have regarding programming for CardLogix smart cards. In some cases we may be able to assist you with your application development or refer you to one of our Smart Partners who may be able to work with you on your programming needs.



ATR 3B 5F 95 00 80 73 00 01 00 59 43 4C 5A C5 06 11 7C 90 00 3B 5F 9

Card Serial Number 12345678

Card Header Information

Card Type	Version	Release Date	Card File Structure
C6	1.01	1/7/2014	WinplexTest.cfs

```
CLX_APIVersion: WinPlex API v4.0.1.6
CLX_OpenReader  OK
ReaderHandle:  1
CLX_ResetReader   OK
CLX_SetCardType:  0
CLX_CardInserted = true
CardOn OK
ATR:3B 5F 95 00 80 73 00 01 00 59 43 4C 5A C5 06 11 7C 90 00
-------------------- Check Files Test ----------------------
CLX_Select7816( 1,2,3D40)  OK
CLX_Select7816( 1,2,3D41)  OK
CLX_Select7816( 1,2,3D42)  OK
CLX_Select7816( 1,2,3D43)  OK
CLX_Select7816( 1,2,3D44)  OK
CLX_Select7816( 1,2,3D45)  OK
CLX_Select7816( 1,2,3D50)  OK
CLX_Select7816( 1,2,3D51)  OK
CLX_Select7816( 1,2,3D52)  OK
CLX_Select7816( 1,2,3D53)  OK
CLX_Select7816( 1,2,3D54)  OK
CLX_Select7816( 1,2,3D55)  OK
-------------------- Read Serial Number --------------------
CLX_Select7816: 3040   0
CLX_ReadBinary7816:    0
-------------------- Read Card Header ----------------------
CLX_Select7816: 3040   0
```

Test Sequence

- 🟩 CardON
- 🟩 Check Files Present
- ☑ 🟩 Read Serial Number
- ☑ 🟩 Read Card Header
- ☑ 🟩 Clear File
- ☑ 🟩 Local CHV
- ☑ 🟩 Master CHV
- ☑ 🟩 Local APP
- ☑ 🟩 Master APP
- ☑ 🟩 DES Encrypted
- ☑ 🟩 3DES Encrypted
- ☑ 🟩 Purse Test
- ☑ 🟩 Local CHV Purse
- ☑ 🟩 Local APP Purse
- ☑ 🟩 Master CHV Purse
- ☑ 🟩 Master APP Purse
- ☑ 🟩 DES Purse
- ☑ 🟩 Internal Auth
- ☑ 🟩 Rehab Test

☑ Select

Figure B.1 *- Winplex® VB 2008 Code Demo*

APPENDIX C: GLOSSARY

Term

Definition.

AC

The acronym for "alternating current".

ACK

The abbreviation for "acknowledge". Used in a communications protocol to acknowledge the receipt of a message.

Answer to Reset

The response an ICC returns when the proper power sequence is applied. Defined in ISO 7816-3 for microprocessor cards. Definition for Synchronous Cards is not as well defined.

APDU

The acronym for Application Protocol Data Unit. It contains either a command message or a response message, sent from the interface device to the card and vice versa.

ASCII

The acronym for "American Standard Code for Information Exchange". It is a character encoding scheme used to represent text in computers.

asynchronous cards

Also known as microprocessor cards. They are ICC's that have a microprocessor and function according to ISO 7816-3 specifications for microprocessor cards. Asynchronous refers to the fact that they communicate using an asynchronous communications technique.

ATR

The acronym for "Answer to Reset".

Authentication

The process of assuring that one, or both, parties involved in a transaction are truly who they declare to be.

BCC

The acronym for "block check character". It is used in many communications protocols to detect errors in transmission.

BPS

The acronym for "bits per second".

Seated Card

Refers to a card that is fully inserted into a card connector, changing the state of the switch inside a reader.

card connector

Any connector designed to receive an ICC.

challenge

Some of the security schemes used with Smart Cards require a random number to be associated with key manipulations. The random number, which of course changes with every transaction/session, assures that no two occurrences of the same transaction will look the same, thus avoiding replay of secure transactions.

CLA

The abbreviation for "class". This is one of the bytes used in an APDU.

communications protocol

A set of rules governing the structure, sequencing, and validation of messages between two or more points on a communications media.

CTS

A hardware signal from the host to the Axiohm model 152 reader which allows the host to block transmission of data coming from the reader.

DB-9

This is the type of connector used to connect to a D-sub 9 port on the host PC.

DC

The acronym for "direct current".

DLL

The acronym for "dynamic link library".

EEPROM

The acronym for electrically erasable programmable read only memory. Most smart cards store user data in EEPROM, which can be erased and reprogrammed numerous times. See the card manufacturer's specifications for information on the number of programming cycles available for a particular card.

EOT

The acronym for "end of transmission". It is a transmission control character used in many communications protocols to indicate the conclusion of a transmission. In the ASCII character set it is defined to have the value 04H.

Erase

In regards to smart cards, "erase" usually means setting data bits to all ones. This is because EEPROM programming changes bits from the erased (all ones) state to zeros one bit at a time, but cannot change single bits from zero to one. Currently available EEPROMs require at least one complete byte to change to ones (erasure) in order to change a single bit to one. Some EEPROMs erase in blocks of 2 or more bytes.

ETX

The acronym for "end of text". This byte is used in many communications protocols to signify the end of a transmission. In the ASCII character set it is defined to have the value of 03H.

F/D ratio

F stands for "frequency", D stands for "divisor". In ISO 7816-3, these terms are used as a ratio (along with an oscillator frequency) to determine the actual speed of the Smart Card interface. ISO 7816-3 defines a default F of 372 with a default D of 1. When used with a standard oscillator frequency a speed of 9600 bps results.

field

An area in the CardAppz® database file that tracks just one type of item, e.g. a city, state, ZIP code, etc.

fuse

Many memory cards have a way of making an irreversible change to the card system so that future modifications to certain portions of the card (e.g. card serial number) are impossible. Usually the technique is referred to as a fuse.

GeldKarte

A variant of the ISO 7816-3, Amendment 1, T=1 protocol.

GSM

The acronym for “global system mobile”, a cell phone card standard.

Hex

The acronym for hexadecimal, base 16. Some numbers in this manual are followed by H (e.g. 03H). This notation is to denote a Hex number.

Host

The device connected to a reader via a communications cable. The host controls all operations of the reader.

ICC

The acronym for “integrated circuit card”. It is any card which acts as a carrier for an integrated circuit. Most particularly, cards which conform to ISO 7816 standards.

INS

Instruction. This is one of the bytes used in a APDU.

ISO 7816

This international standard is used as a guideline by many smart card manufacturers. It defines standards (mechanical, electrical, and operational) for integrated circuit cards with contacts. Other standards apply to ICCs without contacts.

key

Many smart card security schemes require the use of a “key” to prove either a reader has legitimate access to a smart card, or that a reader should accept a smart card as valid.

Lc

One of the parameters which may be used in an APDU, it specifies the length of data being transferred to the smart card.

Le

One of the parameters which may be used in an APDU, it specifies the length of data expected to be returned by a smart card.

LED

The acronym for “light emitting diode”, the visible lights on the front of the reader.

LSAM

The acronym for "local secure application module". A secure application module is inserted in the LSAM connector, located inside the reader.

LSAM connector

This connector (if installed) is found inside the reader where it is not easily accessible to the general public. It receives the LSAM which allows the reader to be used for security applications. One disadvantage of having a SAM in an LSAM connector is the possibility of the whole reader being stolen. Such an occurrence could, if the logical security scheme is inadequate, expose the owner to possible fraud. If the SAM is used to contain actual cash from transactions, the loss of the entire reader could mean loss of the revenue currently residing in the LSAM!

mA

The abbreviation for "milliampere".

memory cards

Also known as "synchronous cards" or "serial cards". These cards do not have a microprocessor. They contain relatively simple circuitry which allows the card to read, write and update data. There are a variety of security mechanisms available on many cards.

microprocessor cards

Also known as "asynchronous cards". ICC Cards which have a microprocessor and function according to ISO 7816-3 specifications for microprocessor cards.

ms

The abbreviation for "milliseconds".

Multi-drop

Refers to techniques that allow for multiple computers/devices to be attached to a single communications line through which they can communicate with each other.

N/A

The abbreviation for "not applicable".

NAK

The abbreviation for "negative acknowledge". This term is usually used when talking about a communications protocol, to designate how one party on a communications line tells another party that a particular message was not received correctly.

OSB

The acronym for "operation status byte". This byte is present in all responses from the reader when using either of the TLP-224 protocols available. It informs the host of the final status of the operation.

P1

One of the parameters used in an APDU. Specific usage depends on the APDU being used.

P2

One of the parameters used in an APDU. Specific usage depends on the APDU being used.

P3

One of the parameters used in an APDU. It is used to indicate that either Lc or Le is being used.

PIN

The acronym for "personal identification number". Many Smart Cards have security mechanisms which presentation of a PIN to authorize usage of the card.

procedure byte

This byte is part of the card level communications for microprocessor cards using the T=0 protocol. It is used to regulate the flow of data from the card to the reader.

record

A collection of fields in a database that defines one entity. (Each card contains 1 record with the exception of the M.O.S.T. Card family).

RFU

The acronym for "reserved for future use". When sending a command to the reader, any field documented as RFU should be filled with zeros.

RS232

An electrical specification of a communications system which is used between parties on a communications line. The Axiohm model 152 reader is RS232 compatible.

SAM

The acronym for "secure application module". Many smart card applications require security to protect against fraud. Many security schemes are implemented via SAMs which are Smart Cards. They make security algorithms available and supply a secure place to store keys.

SAM Box

This accessory, available for connection to many readers, allows the reader access for up to seven additional SAMs. The SAM box may be stored out of sight, in a secure location.

Serial Cards

See "memory cards".

smart card

Any card with implanted, programmable, integrated circuitry.

SOH

The acronym for "start of header". This byte is used in many communications protocols to signify the the start of a transmission. In the ASCII character set it is defined to have the value 01H.

SW1 and SW2

These bytes are defined in ISO 7816 to be the last two bytes of any APDU response. They convey status information about the card operation.

Synchronous Cards

See "memory cards".

T=0

One of the protocols defined in ISO 7816 for communicating with Microprocessor Cards. This protocol is byte oriented, with error correction and recovery techniques applied on a byte-by-byte basis.

T=1

One of the protocols defined in ISO 7816 for communicating with microprocessor cards. This protocol is block oriented, with error correction and recovery techniques applied to entire messages.

TLP-224

One of the communication protocols supported by the Axiohm Model 152 and 171 readers for communications between the reader and the host. This protocol is used by several manufacturers of smart card readers. If you use only the core set of commands in your application, your unit may be plug compatible with units from other manufacturers.

TLP-224 Turbo

A proprietary variant of the TLP-224 communications protocol which reduces the transmission time required to exchange messages between the host and reader.

transport code

A passwording technique used by many manufacturers of smart cards to assure that cards cannot be tampered with, or diverted to other destinations, for fraudulent purposes.

update

This function is used for subsequent writes to an EF that has already been written to previously. Most Smart Cards use EEPROM for data storage, if the new value to be stored at a location has any one bits where the old value had zero bits, the byte (or maybe a larger section of storage space), must be erased prior to writing the new value. In many cards the operation called "update" performs an erase before writing the new value to the card. Consult your card documentation to determine the exact nature of the "update" operation for your card.

user connector

The card connector visible to the user. When the Axiohm model 152 goes through a power cycle, this Connector is selected.

USI2

One of the communications protocols supported by the Axiohm model 152 and 171 readers for communications between the reader and the host. This protocol is unique to American Magnetics. This protocol allows fuller usage of the features of the model 152, 154, and171 readers.

Write

This is the function used when an EF is written for the first time. (All subsequent writes are done via the update function). Most smart cards use EEPROM for data storage, if the new value to be stored at a location has any 1 bit where the old value had zero bits, the byte (or maybe a larger section of storage space) must be erased prior to writing the new value. If the byte is not erased, only bits which change from a 1 to a 0 will be changed. In many cards the operation called "write" only changes 1 bit to 0 bits. Consult your card documentation to determine the exact nature of the "write" operation for your card.

CardLogix Corporation is absolutely committed to providing defect-free products and services to our customers in partnership with equally committed integration partners and authorized resellers.

California C Corporation
CA Resale# SREAA 97 - 124323
D&B# 867418899
SIC Codes# 3577, 3089, 5162
UNSPCSC Code# 32101617
Harmonized Code# 8542.10.0000
NAICS Codes# 334119, 326199, 334418, 334519, 42261, 51421
CAGE Code# 1KV39
Congressional District# 47

16 Hughes, Suite 100 · Irvine, CA 92618 · United States
Phone +1 949 380-1312 · Fax +1 949 380-1428
www.cardlogix.com · sales@cardlogix.com

7000011

ISO 9001:2008 CERTIFIED

CE RoHS COMPLIANT