



Middleware

Issues in Smart Card Development

Simplifying Smart Card Access under Windows a White Paper

Winplex® and PC/SC

Part 3 In A Series

Abstract

In today's business environment there is an increased awareness of security, which is driving smart card application development. The Microsoft® Windows® operating systems are ubiquitous in this environment and some of these operating systems ship with difficult to use base components with no hooks for smart cards. CardLogix has developed an alternative middleware solution to this problem. The CardLogix Winplex API works across all win32 environments. It is easier to develop with, more cost effective and still maintains a complete level of compatibility within the Microsoft architecture.

CONTENTS

INTRODUCTION.....	1
MICROSOFT SMART CARD API.....	2
WINPLEX API.....	3
CONCLUSION	4
ADDITIONAL REFERENCES	5
Resources	5
Documents	5

© 2002 CardLogix Corporation All rights Reserved

This document contains information that represents the present view of CardLogix Corporation on the issues discussed as of the date of publication. Because CardLogix must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Cardlogix, and CardLogix cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. CARDLOGIX MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Winplex is a registered trademark of CardLogix Corporation in the United States and/or other countries.

Other product or company names mentioned herein may be the trademarks of their respective owners.

CardLogix Corporation 16 Hughes • Irvine, CA 92618 • USA

INTRODUCTION

As smart cards are becoming more common, they are being used in more and more applications. Unfortunately, the task of actually building a Windows application that uses a smart card can be quite daunting. If a programmer chooses to work with the base level Microsoft smart card components, they will require the programmer to have a great deal of knowledge of the Microsoft APIs, limit the types of cards the programmer can choose to use, and add unnecessary complexity for the programmer.

CardLogix has developed the Winplex API as an alternative to the Microsoft approach for developing smart card applications under Windows. This API simplifies and speeds smart card access while maintaining support for the Microsoft API. The CardLogix approach also supports third party developer tools such as Borland's Delphi programming language.

MICROSOFT SMART CARD API

Microsoft has defined an API for using smart cards in its operating systems (Windows, 98, 2000, NT, ME, and XP professional) that is based on the Personal Computer/Smart Card (PC/SC) specification (see <http://www.pcscworkgroup.com/>). This interface is quite complex and can be difficult for both experienced and novice programmers. The API (called Scard) requires the programmer to be familiar with the Microsoft Platform Software Development Kit (SDK). The Platform SDK is not a familiar tool to most mainstream programmers and is available only through the Microsoft Developer Network (MSDN) or the Microsoft website. To use the Microsoft API, the programmer must learn things like the name of the reader (instead of the COM port to which it is attached) and the name of the card. Before the programmer can access the card, they must first establish a context with the Scard manager. They must then get a handle to the card. It is only at this point that they can actually access the card to read/write data. Once the programmer is done with the card, they must release the handle to the card and release the context.

The PC/SC specification only defines support for microprocessor cards. For many applications, the use of a microprocessor card is overkill and not cost effective. Also, the PC/SC defined commands represent only a small subset of the commands most smart cards actually support, so special commands (i.e. support for a purse) are only possible by the application developer building their own as Application Protocol Data Units (or APDUs) and sending those down to the card. This requires the programmer to have a detailed understanding of APDU structures and the command specification for the card being supported. If the programmer wants to change to a different card, the APDUs will most likely change requiring more work by the programmer.

When deploying an actual system in a real world environment, the Microsoft API presents some issues. Because of the large number of Windows Operating Systems (95, 98, 2000, NT, ME, XP) and their various flavors and patches, the native operating system support for Scard may be missing or out of date. The installation program for the developed application must be very intelligent to determine what drivers are loaded, their version numbers, what drivers are missing, and then install only the appropriate components.

WINPLEX API

The Winplex API from CardLogix addresses the complexities and deficiencies of the Scard API. Winplex presents a very simple interface to the programmer and has a very rich command set. To add support for an existing application, all the programmer must do is add the appropriate header file and library file (in the case of a C program) or include the proper .BAS file (in the case of the Visual Basic program). Having added these files, talking to the card is simply a matter of opening the reader, reading/writing to the card, and closing the reader. Winplex uses the familiar COM port interface for connecting to a reader. It does not depend on things such as reader names and card names.

Winplex also supports the full line of CardLogix cards and their commands. This allows the programmer to choose on a card type that best fits their application. For those applications that require little storage and little or no security, a memory card may do the trick. Winplex will support all the features of the selected card. If the card requires more memory or more complex features such as on-board encryption, authentication, or password protection, a CardLogix microprocessor card is the better choice (again, completely supported by Winplex). If the programmer wants to use CardLogix's advanced purse features, Winplex simplifies this task.

The Winplex API also supports custom commands for specific readers that PC/SC does not, such as LED indicator control, pin-pad reading, mag-stripe reading, reader card latching, and biometric commands. It also includes simple to execute software encryption/decryption routines for DES, triple-DES, and AES. These algorithms allow the programmer to easily encrypt/decrypt data that is stored on any type of card without the need for developing complex mathematical routines, or developing with additional APIs.

Winplex has also been designed to be fully compatible with the Scard API. A special reader type has been defined in the Winplex OpenReader command that allows the programmer to specify the exact reader they want or to let Winplex use the first reader it determines is connected to the system. The second alternative allows the programmer to build and deploy their application without having to worry about the reader they ship. If the shipped reader changes, the application will still use the first reader found, ignoring the fact that the actual reader name has changed.

Additionally, Winplex simplifies application installation and customer support. The installation program for the end user application only needs to install the Winplex.dll in the appropriate system directory. It does not need to be concerned with the version of Windows or the presence/non-presence of the Scard DLLs and libraries.

CONCLUSION

Microsoft has developed a complex smart card API for some of their Windows Operating Systems. This complexity, and the fact that the Scard API only supports microprocessor cards, makes it difficult to use and limits the card choices for the programmer and their issuer. To overcome these deficiencies, CardLogix has developed the Wimplex API. Wimplex simplifies the interface for the programmer, adds support for non-microprocessor cards, takes advantage of reader specific functions and increases the native command set for cards. It does all of these things while maintaining a PC/SC compatible interface for those customers that require PC/SC.

ADDITIONAL REFERENCES

Resources

CardLogix Corporation

<http://www.cardlogix.com>

Smart Card Basics

<http://www.smartcardbasics.com>

Microsoft Test Certificate Server:

<http://sectest.microsoft.com/>

Documents

Microsoft CryptoAPI and other public-key technologies:

<http://www.microsoft.com/security/>