

# Xtreme PC Smart Card Solutions

## White Paper

Written By: *Moshe Chen*

---

### Abstract

Chip PC provides variety of Smart Card Solutions for authenticating users to windows 2000 domain and setting of connection list based on user credentials. Authentication using Smart Card can be implemented in three different ways: The first is *Smart Card Standard PKI Log On* involving Xtreme PC Thin Client, Active Directory, Kerberos Protocol and Public Key Certificates. The second is *Chip PC Log On* which can be used in one of two ways: The first is *Smart Card Local Login* which involves Xtreme PC Thin Client, Smart Card Local Login XPI and Smart Card. The Second is *Smart Card User Login* which involves Xtreme PC Thin Client, Active Directory, Xcalibur Management Software and Smart Card. The third way is the *Unified Smart Card Log On*, involving Xtreme PC Thin Client, Active Directory, Kerberos Protocol, Xcalibur Management Software and Smart Card. Chip PC's Xtreme PC with a build-In PC/SC Smart Card reader offer the customers with increased level of security, portability of credentials and other private information between Xtreme PC Thin Client devices in addition to automatic connection setting based on user credentials.

---

© 2004 Chip PC Inc., Chip PC (Israel) Ltd. All rights reserved.

*The information contained in this document represents the current view of Chip PC on the issues discussed as of the date of publication. Because Chip PC must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Chip PC, and Chip PC cannot guarantee the accuracy of any information presented after the date of publication.*

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

*Xcalibur, Chip PC and the Chip PC logo are either trademarks or registered trademarks of Chip PC.*

*Products mentioned in this document may be registered trademarks or trademarks of their respective owners.*

---

## CONTENTS

|  |          |
|--|----------|
| <b>INTRODUCTION .....</b>  | <b>1</b> |
| PC/SC PKI Smart Card Solutions for Markets Requiring High-Security (e.g. Healthcare, Government) | 1        |
| Log On Process   | 1        |
| Smart Card Benefits  | 1        |
| <b>QUICK TERMS GUIDE .....</b>   | <b>2</b> |
| What is a Smart Card?  | 2        |
| What is Cryptography?  | 2        |
| Public Key Cryptography (PKI)  | 2        |
| Certificate  | 3        |
| Kerberos   | 3        |
| <b>XTREME PC SMART CARD SOLUTIONS.....</b>   | <b>4</b> |
| Preface  | 4        |
| Terms  | 4        |
| <b>STANDARD PKI SMART CARD SOLUTION .....</b>  | <b>5</b> |
| Functionality  | 5        |
| How It Works?  | 5        |
| Required Components  | 5        |
| General  | 5        |
| Smart Card   | 5        |
| <b>CHIP PC SMART CARD SOLUTIONS.....</b>   | <b>6</b> |
| Preface  | 6        |
| Smart Card Solutions   | 6        |
| 1.1 Smart Card Local Login   | 6        |
| Functionality  | 6        |
| How It Works?  | 6        |
| Required Components  | 6        |
| 1.2 Smart Card User Login  | 7        |
| Functionality  | 7        |
| How It Works?  | 7        |
| Required Components  | 7        |
| <b>UNIFIED SMART CARD SOLUTION (PKI &amp; CHIP PC).....</b>                                      | <b>8</b> |
| Preface  | 8        |
| Functionality  | 8        |
| How It Works?  | 8        |
| Required Components  | 8        |

---

---

## INTRODUCTION

### **PC/SC PKI Smart Card Solutions for Markets Requiring High-Security (e.g. Healthcare, Government)**

Signaling a major industry push towards stronger client security, Chip PC now offers thin clients with complete PC/SC PKI smart card solutions. Smart cards, containing processing power and memory to store data, are often used as a form of identification and access. Organizations in fields such as healthcare, finance and government use smart cards to provide employees with access to secure buildings and confidential information and applications.

Chip PC thin clients now provide integrated smart card readers and support external smart card readers working with the industry-standard PC/SC protocol and under PKI environments, built-in into Microsoft servers.

In addition to supporting Industry-standard PKI smart card solutions, Chip PC offers smart card applications and management at the local and server levels combined with the Xcalibur comprehensive management software.

With Chip PC smart card solutions, the same card may be used for Windows Authentication in PKI environment as well as for secured access Smart Card applications.

Chip PC smart card solution offers both flexibility and comprehensiveness. The user may choose any combination of PKI authentication, local login into device with PIN code and User login where connections are retrieved from the server according to Users & Groups information stored in the Xcalibur management software.

### **Log On Process**

A key feature of Microsoft Windows 2000 authentication is its support of single Log On. Single Log On simplifies security administration and allows a user to Log On to the Domain once, by using a single password or Smart Card, automatically authenticating to any computer in the Domain. However, single Log On also increases the need to secure the Log On process. Smart Cards provide an additional layer of security for the Log On process.

### **Smart Card Benefits**

The use of Smart Card increases the security of the Log On process by providing:

- Tamper-resistant storage for protecting private keys and other forms of private information.
- Isolation of security critical computations from other parts of the system.
- Portability of Credentials and other private information.

---

## QUICK TERMS GUIDE

### What is a Smart Card?

The term *smart card* has been used to describe a class of credit card-sized devices with varying capabilities: stored-value cards, contact-less cards, and integrated circuit cards (ICC). All of these cards differ in functionality from each other and from the more familiar magnetic-stripe cards used by standard credit, debit, and ATM cards. It is the ICC that is of most interest to the personal computer, and Windows 2000, because it is able to perform more sophisticated operations such as digital signature and key exchange.

A smart card is essentially a miniature computer, embedded in plastic in the form of a credit card, with limited storage and processing capability. The circuitry in a smart card derives power from a smart card reader after the card is inserted into the reader. Data communication between a smart card and an application running on a computer is performed over a half-duplex serial interface managed by the smart card reader and its associated device driver.

### What is Cryptography?

Cryptography is the science of protecting data or messages. Many cryptographic algorithms mathematically combine input plaintext data and an encryption key to generate encrypted data referred to as *ciphertext*. With a good cryptographic algorithm, it is computationally infeasible to reverse the encryption process and derive the plaintext data from the ciphertext. In order to decrypt the ciphertext some additional data, a decryption key, is needed to perform the transformation.

In traditional secret (or symmetric) key cryptography, encryption and decryption keys are identical and must be shared by multiple parties. Parties wishing to communicate with secret-key cryptography must securely exchange the encryption/decryption keys before they can exchange encrypted data.

### Public Key Cryptography (PKI)

In contrast, the fundamental property of public-key (PK) cryptography is that the encryption and decryption keys are different. Encryption with a public key is a one-way function; plaintext turns into ciphertext, but the encryption key is unrelated to the decryption process. A decryption operation requires a private key (related, but not identical, to the encryption key) to transform the ciphertext back into plaintext. Therefore, every public key user has a pair of keys consisting of a public key and a private key. By making the public key available to anyone, it is possible to enable someone to send encrypted data to another person (or persons) that can only be decrypted by the recipient using the private key. Separation of the public key from the private key has enabled new applications of cryptography such as digital signature, key agreement, and distributed authentication.

Authentication typically requires some type of challenge-response between authenticating parties. Public key cryptography provides a means by which a challenge-response can be accomplished between two parties who have never met

---

because the public key and private key are distinct and separate. Separation of the private and public key enables distributed authentication because it does not require that the parties share a key *a priori*. Likewise, public key cryptography can also be used to generate a shared key without the parties having to meet in secret.

In addition, data can be transformed using a private key in such a way that recipients can verify the data originated from a specific sender and that the data has not been tampered with while in transit. This is known as *digital signature* and is quite powerful. Digital signatures are themselves just data so they can be transported along with the signed data that they protect. A *digital signature* ensures identity because only the owner of the private key could have signed the data, and integrity because modification of the data after it is signed invalidates the signature. Anyone can verify a signature because the public key can be published in a directory as part of a certificate.

### **Certificate**

Public Key are required for PKI based security, they are usually packaged as digital certificates (Only Public Key are packaged in to certificates. The private key is never shared, so it doesn't require packaging – it's simply stored securely). The certificate contains the Public Key and a set of attributes, like the key holder's name. These attributes maybe related to the holders identity, what they are allowed to do, or under what conditions the certificate is valid. The binding between attributes and Public Key is preset because the certificate is digitally signed by the entity that issued it. The issuer's signature on the certificate vouches for its authenticity and correctness. In the certificate authentication process, your computer presents its certificate to the server, and the server presents its certificate to your computer, enabling mutual authentication.

The certificate is stored on the Smart card.

### **Kerberos**

The Kerberos authentication protocol provides a mechanism for mutual authentication between a client and a server.

---

## **XTREME PC SMART CARD SOLUTIONS**

### **Preface**

Chip PC provides three types of Smart Card solutions with its innovative Xtreme PC Thin Clients:

1. Standard PKI Smart Card Solution.
2. Chip PC Smart Card Solution.
3. Unified Smart Card Solution (PKI & Chip PC).

### **Terms**

A user can basically perform two actions on any thin client. First is configuring local *connections* and second is configuring *local hardware settings*.

**Connection** – Client side application which is used to connect to network services (RDP, ICA, Local Browser, Terminal Emulation).

**Local hardware Settings** – Xtreme PC's local setting like: display resolution, network setting, local printers, keyboard ...

---

## **STANDARD PKI SMART CARD SOLUTION**

### **Functionality**

Authenticate a user to a windows 2000 domain securely by using Smart Card and Xtreme PC Thin Client with build-in (Or external) PC/SC Smart Card reader.

### **How It Works?**

Log On by using Smart card begins when at the end of the Xtreme PC boot process the user uses one of the RDP or ICA connections to connect to a terminal server. Once connected, the user is prompted with the *Insert Smart Card* logon dialog box. The user inserts a Smart Card into the Xtreme PC's Smart Card reader. The insertion of the Smart Card signals the windows 2000 operating system to prompt for a PIN Code instead of a User Name, Password and Domain Name. Once the PIN Code is provided the certificate that is stored on the Smart Card is read and used for the authentication of the card holder to the domain.

### **Required Components**

#### **General**

- Xtreme PC Device with built-in Smart Card Reader: Models 5052, 5452, 5652.
- External Smart Card Reader (Optional) Chip PC P/N: **CPN01488**.

#### **Smart Card**

In order to implement Standard PKI Smart Card Solution the user has two options regarding the type of the Smart Card:

1. SCSQUARE ([www.scsquare.com](http://www.scsquare.com)) PKI Smart Card – Purchase the card from Chip PC (P/N: **CPN01517**).
2. Any Standard PKI Smart Card– Use any standard PKI Smart Card in the market which is purchased directly from the manufacturer of the card.

---

## CHIP PC SMART CARD SOLUTIONS

### Preface

Chip PC provides NEW innovative and incomparable Smart Card solution with its Xtreme PC Thin Client that offers increased security, manageability and flexibility.

### Smart Card Solutions

Chip PC provide two types of Smart Card solutions:

1. Smart Card Local Login.
2. Smart Card User Login.

## 1.1 Smart Card Local Login

### Functionality

Provide the user with a secure access to the Xtreme PC Thin Client by inserting physical Smart Card and providing the appropriate PIN Code.

### How It Works?

A user powers on the Xtreme PC device and receives the *Insert Smart Card* dialog at the end of its boot process. Once the user inserts his Smart Card he is prompted to type the card's PIN Code in order to receive access to the device. Once the PIN Code is provided the user is displayed with the available local connection list (RDP and ICA connections).

Note: The PIN Code the user provides is used to authenticate only the Smart Card and not to the domain itself.

### Required Components

- Device with built-in Smart Card Reader: Models 5052, 5452, 5652.
- External Smart Card Reader (Optional) - Chip PC P/N: **CPN01488**
- Smart Card Local Login XPI (Chip PC P/N: **CXP01542**).
- SCSQUARE ([www.scsquare.com](http://www.scsquare.com)) PKI smart card - Purchase from Chip PC (Apollo PKI Smart Card, Chip PC P/N: **CPN01517**).
- At least one Smart Card Manager XPI (for programming Smart Card PIN code) – (Chip PC P/N: **CXP00867**).

---

## 1.2 Smart Card User Login

### Functionality

Set a list of available *connections* automatically to the Xtreme PC device based on user credentials from the Xcalibur Management software.

### How It Works?

A user powers on the Xtreme PC device and receives the Insert Smart card dialog at the end of its boot process. Once the user inserts his Smart Card he is prompted to provide the card's PIN Code. Once provided the user credentials are read from the card and sent to the domain controller for validation. Once validated, the user credentials are sent to the Xcalibur Management System. The Xcalibur checks its database and configures the Xtreme PC device with a list of connections according to the user credentials.

### Required Components

- Device with built-in Smart Card Reader: Models 5052, 5452, 5652.
- External Smart Card Reader (Optional) - Chip PC P/N: **CPN01488**
- SCSQUARE ([www.scsquare.com](http://www.scsquare.com)) PKI smart card - Purchase from Chip PC (Apollo PKI Smart Card, Chip PC P/N: **CPN01517**).
- Smart Card User Login XPI (Chip PC P/N: **CXP01542**).
- Xcalibur Management Software - (Chip PC P/N: **CPN01519**).
- At least one Smart Card Manager XPI (for programming Smart Card PIN code and user credentials) – (Chip PC P/N: **CXP00867**).

---

## UNIFIED SMART CARD SOLUTION (PKI & CHIP PC)

### Preface

Chip PC's Xtreme PC Thin Client with the build in PC/SC Smart Card reader provides incomparable Smart Card solution which combines the previous two solutions into one Unified Smart Card Solution.

### Functionality

The Unified Smart Card Solution offers the following:

1. Authenticate a user to a windows 2000 domain securely by using Smart Card and Xtreme PC Thin Client with build-in (Or external) PC/SC Smart Card reader.
2. Set a list of available *connections* automatically to the Xtreme PC device based on user credentials from the Xcalibur Management Software.

### How It Works?

A user powers on the Xtreme PC device and receives the Insert Smart card dialog at the end of its boot process. Once the user inserts his Smart Card, the Xtreme PC's *connection manager* is presented with the list of the user's *connections* retrieved from the Xcalibur Management Server. The user chooses one of the connections to connect to a terminal server. Once connected the user is prompted to provide PIN Code. Once provided the certificate that is stored on the Smart Card is read and used for a secure authentication of the card holder to the domain.

### Required Components

- Device with built-in Smart Card Reader: Models 5052, 5452, 5652.
- External Smart Card Reader (Optional) - Chip PC P/N: **CPN01488**
- PC/SC Smart Card User Login PKI - (Chip PC P/N: **CXP01542**).
- SCSQUARE (www.scsquare.com) PKI Smart Card - Purchase from Chip PC (Apollo PKI Smart Card, Chip PC P/N: **CPN01517**)
- SCSQUARE CSP (Cryptographic-Service-Provider) – provided by Smart Card Manufacturer (SC Square).
- At Least one Smart Card Manager XPI (for programming Smart Card PIN code) - Chip PC P/N: **CXP00867**.
- Xcalibur Management Software - (Chip PC P/N: **CPN01519**).