

**CHARGE Anywhere
Secure Payment Solutions
Client Implementation Document**



**Last Revision: 3/18/2009
Version M**

Revision #	Date	Name	Description
1	11/08/07	CP	Added sections 13 and 14
2	11/12/07	CP	Updated section 12 to include recommendations for browser security.
3	11/15/07	CP	Reviewed all sections
4	11/20/07	CP	Updated section 12 and added section 15
5	11/30/07	CP	Updated section 12 to include Storage card information
6	1/15/08	CP	Added section regarding key rotation and troubleshooting procedures
7	3/17/08	CP	Removed sections that are no longer relevant
8	5/02/08	CP	Modified the section related to WiFi configuration
9	6/04/08	CP	Added wording regarding upgrades.
10	11/24/08	CP	Updated uninstall section for J2ME device
11	3/18/09	CP	Added the User Management section

1.	How to create Passwords.....	4
2.	Secure Transmission of Data.....	5
3.	Secure Access to systems with cardholder data	7
4.	Secure Wireless(WiFi) Setup	8
5.	Configuring WiFi(VeriFone Only).....	9
6.	Application of Security Updates.....	10
7.	Key Maintenance.....	11
8.	Compromised Key Procedures	12
9.	Implementing Mobile Phone Security.....	13
10.	Security Guidelines for 3 rd Party Mobile Phone Applications.....	14
11.	Secure Storage of Non-Truncated Receipts.....	15
12.	Uninstall procedures	16
13.	Upgrade Procedures.....	17
14.	Training Sessions	18
15.	Troubleshooting Procedures	19

WARNING: If all recommendations in this guide are not followed the application will not be PABP compliant.

1. How to create Passwords

The following guidelines pertain to PABP requirement 3.1.

The application utilizes 3 types of passwords:

- Application Password
- Transaction Password
- Manager Password

The default password for all three types of passwords is '12345678'.

The user is **required to change** all default passwords the first time he enters the app. He can do so by going to **Security/Password Options**.

Passwords expire every **90** days and the user is required to change them.

User can not reuse any one of the last 4 passwords within the same password type.

Application uses strong password policy described below.

Password Policy:

- Password has to be at least 8 alphanumeric characters
- Password must have digits
- Password must have both upper and lower case letters
- Password has to have at least 4 letters
- Password has to have at least 3 digits
- Immediate occurrence of same alphanumeric not allowed. ex: 25bb7eM9ru is not a valid password; "bb" not allowed
- Letter Sequence forward or backward not allowed. ex: 1cd5M9d54 and 1fe5M9d54 are not a valid passwords; "cd" and "fe" are not allowed.
- Digit Sequence forward or backward not allowed. ex: b12u5M9d54 and b43u5M9d54 are not a valid passwords; "12" and "43" are not allowed
- More than 3 same Letters not allowed
- More than 2 same Digits not allowed

Every time user restarts the device and enters the application, the application will inform the user if he is using default/expired passwords. It is the responsibly of the user to immediately change the default passwords, and to changes the expired passwords.

Please note that when you are entering the password, you will be able to see what you are entering however, when you are entering the password on any other screen, your password will be masked (you will see asterisks).

Also, when you enter a screen to change a password, you will see your password since you have just entered it, so it is no secret at this point.

Application Password and Manager Passwords are required, where the Transaction Passwords are not required. User can turn on the option of asking for a password per transaction from **Security/Transaction Security**. However the Transaction Password is still subject to all above specifications.

2. User Management(CHARGE Anywhere for Windows)

When starting the application for the first time, you will be presented with a screen to set the password on the “Owner” account, this password should follow the guidelines of Section 1. This account is required and has access to all the functionality available within the application.

User accounts should be created by logging in with the “Owner” account or an account with the User Management privileges. The following steps should be followed to create a new user:

NOTE: If creating a user that is only going to run transactions, it is recommended to extend the Idle Timeout.

1. Sign in with an account that has the appropriate privileges
2. Right click on the CHARGE Anywhere icon in the system tray
3. Select **User Management**
4. Select **Add User**
5. Fill in the **Username**
6. Assign a **Password**
7. Assign a **Clerk Number**
8. Revise the **Idle Timeout** is required
9. Select a **Permission Template** or check the desired permissions
10. Press **Create**

3. Secure Transmission of Data

Data must be sent using the SSL protocol to meet PABP requirement 12.1. This is the default used by the application.

4. Secure Access to systems with cardholder data

Use unique username and complex passwords to access machines with payment applications and/or cardholder data per PABP requirement 3.1.

All devices that hold card data must be accessed with a complex password. Please follow the same guidelines as in section 1: "How to create passwords".

Default passwords must be changed immediately upon the user's next login.

Keep passwords secure. Authorized users are responsible for the security of their passwords and accounts. These passwords must be changed every 90 days.

5. Secure Wireless(WiFi) Setup

CISP-compliant wireless settings for deployment of a payment application in a customer environment per PABP 6.1.

Wireless POS solutions are permitted to be deployed at a customer's facility. The wireless POS communicates directly with the customer's access point and data is then routed to CHARGE Anywhere's data center via the internet in a VISA/Master card approved encrypted methodology.

The following configuration steps **MUST** be used as the basis for all Wireless Access Point (WAP) system deployments:

- Change the default SSID (Service Set ID or network name)
- Disable the SSID broadcast
- Change the default password for the WAP's Administrator account
- Enable MAC Address Filtering
- Limit the number of allowed connections to the minimum needed
- Disable DHCP
- Enable the highest encryption possible:
 - WPA with TKIP or AES (802.11g)
 - WEP 128-bit (802.11b)
 - Only to be used if WPA is not available and the following guidelines **MUST** be adhered to:
 - Shared WEP keys must be rotated at least quarterly
 - Shared WEP keys must be rotated whenever there are changes to personnel with access to keys
- Enable the WAP's firewall
- Disable the 'DMZ' feature
- Disable the Remote Management feature
- Disable Universal Plug 'n' Play (UPnP) feature
- Place the WAP near the center of buildings and avoid placing near exterior walls

Under no circumstances should the encryption strength be configured to be less than 128 bits. Wireless encryption keys will be changed periodically, or whenever an administrator with knowledge of the keys is terminated.

6. Configuring WiFi(VeriFone Only)

The MAC address of the terminal can be found on the box that the terminal was received in, or by using the status menu in the Comm Server application and printing out the settings listed there.

1. Enter the Comm Server application
2. Press the leftmost purple button above the keypad
3. Press the rightmost purple button above the keypad
4. The status information will print.

The procedure listed below are the steps required to configure the VeriFone Comm Server application to use a specific access point and to enable encryption.

1. Enter the **CommServer** application
2. Select the **Cfg** option
3. Select the **WiFi** option
4. Press F3 to enter the **Network Name** (This is the SSID)
5. Scroll down to **Encryption**
6. Press F3 to edit the encryption method
7. Press F3 to select **128-bit** encryption
8. Scroll down to **Network Key 1**
9. Press F3 to enter in the first network key that is in use by the Access Point
10. Scroll down to **Network Key 2**
11. Press F3 to enter in the second network key that is in use by the Access Point
12. Scroll down to **Network Key 3**
13. Press F3 to enter in the third network key that is in use by the Access Point
14. Scroll down to **Network Key 4**
15. Press F3 to enter in the fourth network key that is in use by the Access Point
16. Scroll down to **Key Index**
17. Press F3 to edit
18. Enter the value of "1"
19. Press F4 to exit
20. Press F1 to save changes
21. CommServer will restart and take the new settings into use

7. Application of Security Updates

All CHARGE Anywhere customers, Resellers, System integrators must apply security updates to their systems as available. In the event that there is a security related update that is required of the application an email will be sent to the effected parties. There will also be an announcement posted on the main site.

The communications will contain instructions on what actions need to be taken to update the effected pieces of software.

8. Key Maintenance

It is required that the merchant perform a key rotation from the maintenance menu at least once per year. The recommendation is that the key rotation be performed on a quarterly basis. The steps required to rotate keys follows:

- Launch the application
- Enter the required password
- Select Maintenance from the Main Screen
- Enter the required password
- Select Rotate KEK
- Select Rotate Keys

9. Compromised Key Procedures

In the event that the merchant suspects or knows that their key has been compromised, a key rotation must be performed immediately to prevent the disclosure of sensitive data. To rotate the keys, follow the steps that are detailed in the section labeled Key Maintenance.

10. Implementing Mobile Phone Security

Instruct customers on how to harden a mobile phone being used as a credit card processing device. The instructions should also include instructions/information pertaining to external devices, such as a Bluetooth card reader.

Treo®(Windows®):

NOTE: The application will NOT launch from the Storage card.

It is advised that all customers follow these procedures to harden their mobile device to prevent unauthorized access. The following steps should be taken:

1. Go to Start Menu →Settings →Connections Tab
2. Tap Bluetooth
3. Check the box labeled “Turn on Bluetooth”
4. Uncheck the box labeled “Make this device discoverable to other devices”
5. Tap the Security Tab
6. Check the box labeled “Authentication(Passkey) required”
7. Tap OK

It is recommended that the device should have a password set to prevent unauthorized use. In this section if the option is available on the device, select the option to enable strong alphanumeric passwords. This feature can be accessed from the following screen:

Start Menu→Settings→Personal Tab→Password

After the password is set, set the device inactivity timer. This feature can be accessed from the following screen: Start Menu → Settings → System Tab → Power → Advanced Tab
Set the two options listed there to be checked and that the time is set to 15 minutes or less.

It is also recommended that the user make the following changes to the Internet Explorer web browser on the mobile device:

1. Open Internet Explorer
2. Tap Menu
3. Go to Tools... → Options
4. Tap the Security Tab
5. Uncheck “Allow Cookies”
6. Check “Warn when changing to a page that is not secure”
7. Tap OK

These changes are recommended to prevent any accidental disclosure of personal data due to browsing to a malicious site. Please read all warnings presented carefully before continuing to make sure that the page that was arrived at is indeed the page that you intended to visit.

Special Notes Regarding the P25M Card Reader:

The P25M has a security feature that once it is paired to a mobile device, it is no longer discoverable by any other mobile device. This prevents the data from being transmitted to multiple devices. Each P25M has an eight digit passkey that is unique to each device and is required to pair to a mobile device.

11. Security Guidelines for 3rd Party Mobile Phone Applications

Special Note regarding installing 3rd party applications onto your mobile phone

It is advised that the user restrict the 3rd applications that are installed onto the mobile phone to those that are trusted. It is recommended if a 3rd party application must be loaded, that the user verifies that it is a signed application from a reliable source. If these guidelines are not followed, a trojan or other form of malware may be inadvertently installed and compromise the security of the device.

12. Secure Storage of Non-Truncated Receipts

Special Notes on receipt truncation options

When the application is configured to not truncate the merchant copy of the receipt, this receipt must be stored in a secure manner. For example, in a safe that only the manager has access to. This procedure is imperative as failing to do so could lead to the compromise of card holder data.

13. Uninstall procedures

Treo(Windows):

The merchant must uninstall the software when no longer needed or when an upgrade is to take place. The uninstall process will delete all historical data (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software). This process is absolutely necessary for PABP/PCI compliance.

Uninstall procedure:

1. Go to Start Menu → Programs → File Explorer
2. Navigate to “\Program Files\ChargeAnywhere\”
3. Tap on “Uninstaller”
4. Tap on the “Uninstall” option
5. Select “Yes” to remove the application
6. Tap “Exit”
7. Close File Explorer
8. Go to Start Menu → Settings → System Tab → Remove Programs
9. Select “CHARGE Anywhere”
10. Tap “Remove”

J2ME:

Uninstall procedure:

1. Navigate to the application area for the model of phone in question
2. Highlight the CHARGE Anywhere application
3. Select “Options”
4. Choose the “Delete” or “Uninstall” option
5. Choose “Yes” if asked to confirm application removal
6. Follow any further instructions that are presented by phone

14. Upgrade Procedures

VeriFone:

The upgrade procedure for the VeriFone device involves performing a download from the VeriCentre server, maintained by CHARGE Anywhere, to the terminal. The only option that is supported is a Full download from the server. This process removes all historic data and cryptographic material from the terminal per PABP requirements. The application resides in a private group that only contains the CHARGE Anywhere application and is not accessible by other applications. The group is specified by the VeriCentre server and cannot be modified by the user.

15. Training Sessions

Training sessions will be held periodically per PABP requirement section 14. The session information will be sent out in an email two weeks prior to the scheduled date of the training. The training will cover the PABP requirements to deploy the payment application in a secure manner.

16. Troubleshooting Procedures

During the troubleshooting of a device, the data on the device will not be copied nor transmitted in any fashion. The troubleshooting process involves a customer support representative directing the merchant to take specific steps to remedy the issue. If the customer support representative cannot resolve the issue, they document the exact error and if possible the steps required to recreate it. The issue is then posted to the development team. The development team tries to reproduce the issue, resolves it, and then publishes a new version for download.

The steps described above also apply to any reseller's or integrator's support staff. Under no circumstances should application data be copied from the device or transmitted in any fashion.

About CHARGE Anywhere: CHARGE Anywhere is a leading provider of secure Point of Sale (POS) solutions and electronic payment services. Our proprietary Visa Payment Application Best Practices (PABP) Charge Anywhere® v2.0.0 Mobile Payment and POS software solution designed for QuickBooks®, Smartphones and e-commerce environments, and the Web Terminal Payment Solution - ensures Payment Card Industry (PCI) Level 1 compliance via ComsGate® Payment Gateway. CHARGE Anywhere offers business partners and customers the most secure and robust selection of industry specific and customized POS solutions and services, including; IP/Wireless Payment Gateway, POS software, Encryption and Data Security Services, Custom Card Issuance, and Merchant Billing Services. For more information contact them at www.chargeanywhere.com , or (800) 211-1256.