Advanced Card Systems Ltd.
Card & Reader Technologies

APG8202 PINhandy 2 One-time Password Generator

User Manual

info@acs.com.hk
www.acs.com.hk

Table of Contents

Figures

Tables

1.0. Getting Started

1.1. Device Description

The **PINhandy Series** is a family of dynamic password generators created to perform secure authentication in various applications. It is a portable and low-cost handheld smart card device that is capable of managing One Time Passwords, Challenge-response Authentication Codes, and Transaction Data Signing (PKI digital signatures) based on the security keys stored in the EMV cards. The **PINhandy** is compliant with major banking, computing and safety standards such as Mastercard® Chip Authentication Program (**CAP**), MasterCard® Advanced Authentication for Chip (**AA4C/PLA**), VISA Dynamic Passcode Authentication (**DPA**) and **EMV Level 1**.

The APG8202 PINhandy 2 is a compact and completely standalone OTP (One-time password) generator that contains a keypad and a display. It uses two-factor authentication which requires the cardholder to insert the EMV card (*something you have*) into the device and enter a PIN (*something you know*) using the built-in pin-pad. The display screen will then let somebody see a generated dynamic one-time password, which can be used to perform secure online transactions, telephone orders or e-banking logons.

In addition, the **APG8202 PINhandy 2** has no physical connection to a separate device like a PC. Thus, the unconnected mode of the device makes it impossible for hackers to steal the sensitive information stored in the card.

1.2. Supported Card Type

- CAP certified EMV contact card, including:
  a. M/Chip Lite 2.1 with CAP personalization profile
  b. M/Chip 4 with CAP personalization profile
  c. M/Chip Select 2.05 with CAP personalization profile
- PLA/AA4C certified EMV contact card
- VISA DPA certified contact card

1.3. Supported Language

- English
- French
- Traditional Chinese
- Simplified Chinese

2.0. APG8202 PINhandy 2

2.1. Device and Parts

Figure 1 shows the different parts of the APG8202 PINhandy 2 and their descriptions. Figure 2 shows the string holder, which is located at the bottom left corner of the device.

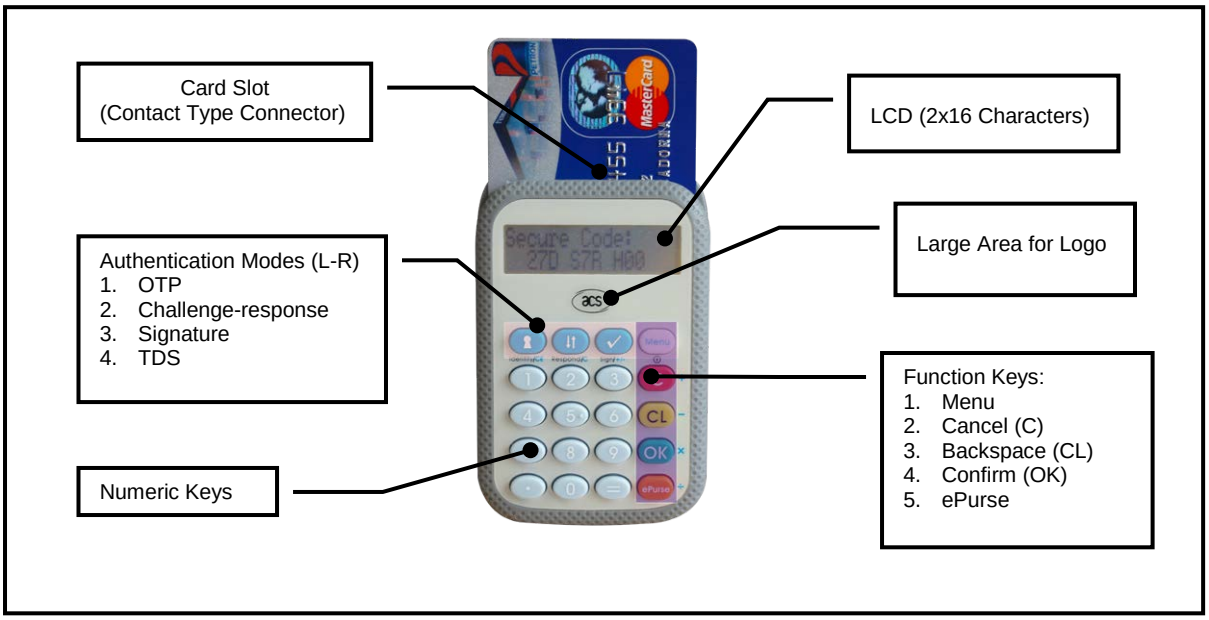
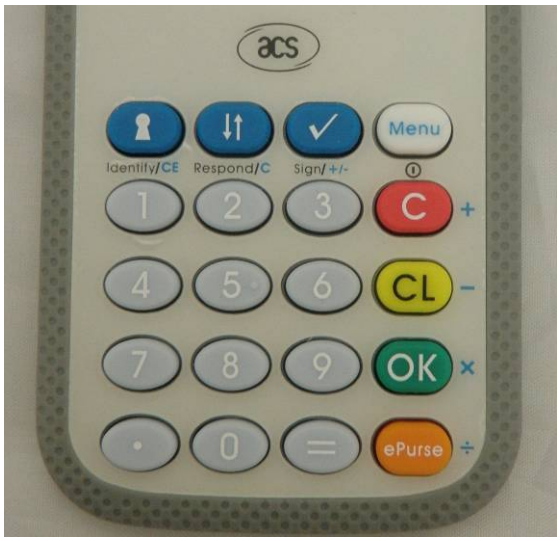


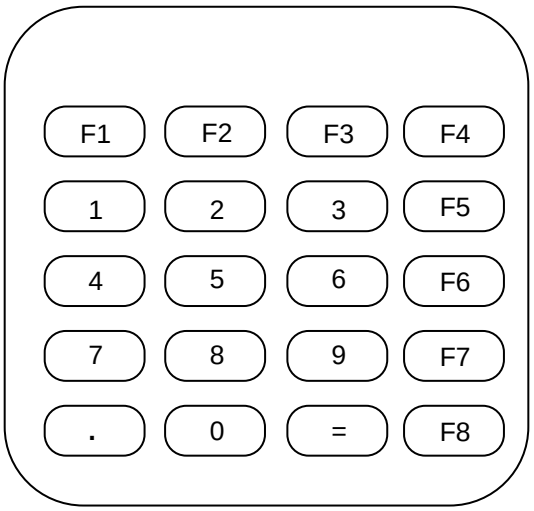
Figure 1: APG8202 Main Components

Figure 2: APG8202 String Holder

2.2. Function Keys

The function keys of the APG8202 for the Normal Mode and the Calculator Mode are described in the table below.





	Normal Mode	Calculator Mode
F1	Hot Key for Identify	Clear
F2	Hot Key for Respond	Cancel
F3	Hot Key for Sign	+/-
F4	Press: Function Select Hold: Power: On/Off	Exit Calculator function
F5	Cancel	Add (+)
F6	Clear	Subtract (-)
F7	Enter	Multiply (x)
F8	ePurse	Divide (/)

Table 1: Function Keys in Normal Mode and Calculator Mode

3.0. Four Authentication Modes of PINhandy

PINhandy has four authentication modes: **Identify, Respond, Sign** and **Advanced Sign** modes. During real transaction, cardholder selects the mode to be executed, which is usually instructed by the authentication form on the Internet. (e.g. '*Insert your payment card and select the Identify mode on your personal card reader to log on to your bank account*')

- **Identify mode** - This mode can be used where one-time passwords are required. No challenge, amount, or currency data is needed when using the APG8202. It may be used to generate the one-time password for e-banking login.

- **Sign mode -** This mode provides a cardholder authentication function. It requires the cardholder to input a challenge value (a set of decimal number of up to eight digits, usually provided by the Online authentication form), and, depending on the configuration of the card in use, the transaction amount and/or currency. It allows issuers to have the option to sign a challenge value for services that involve amount and currency, like in an e-commerce application.

- **Respond mode** - This mode can be used to implement challenge-response authentication. This mode functions in exactly the same way as Sign mode, but it does not require the input of currency and amount values. It allows issuers to have the option to sign a challenge value for services that do not involve amount and currency. For example, to login an online banking account.

- **Advanced Sign mode** - This mode connects the CAP token more closely with a specific transaction and can be used for signing a particular payment. It requires the cardholder to input the transaction data (e.g. the account number of person you are paying) into the card reader, which may be supplied to the cardholder on the Internet authentication form, or by the cardholder on the submitted form. The purpose of this mode is to obtain explicit cardholder approval of the transaction data.

4.0. Frequently Asked Questions

Q: How do I abort a transaction?

A: You can always abort the transaction by pressing **<C>**. Menu page will be displayed again.

Q: What should I do if there is no response from PINhandy after card insertion?

A: You can remove the card for a few seconds, and then re-insert it to the PINhandy. If it still does not work, check if the batteries are out of power.

Q: How do I insert or replace the battery of the PINhandy?

A: The battery of the PINhandy could be replaced or inserted through the following steps:

1. Pull out the battery case.
2. Insert two CR2032 batteries into the battery compartment.
3. Plug in the battery case.

Figure 3: APG8202 with Battery Taken Out

5.0. Glossary

- OTP – One-time Password
- CAP – Chip Authentication Program
- PLA – PIN-/Perso-less Authentication
- AA4C – Advanced Authentication for Chip
- DPA – Dynamic Passcode Authentication
- ATC – Application Transaction Counter
- M/Chip – MasterCard Chip

6.0. Technical Support

For any questions and inquiries regarding the product, please send an email to info@acs.com.hk