Advanced Card Systems Ltd.
Card & Reader Technologies

APG82 PINhandy

One-Time Password Generator

A Product Presentation

www.acs.com.hk

Rundown

1. Product Overview
2. Product Feature
3. Product Value
4. Product Application
5. Q & A

Product Overview

What is a One-Time Password (OTP)?

Passwords that can only be used ONCE

It can be predefined (list) or randomly generated

Benefits of OTP

More secure – difficult to hack or phish

No need to remember multiple passwords for different systems

Unique set of passwords for different people

PIN	vs	OTP
Static Password		Dynamic Password
Remember many passwords		Remember little or no passwords
Set of passwords is personalized		2 people can never have the same set of passwords

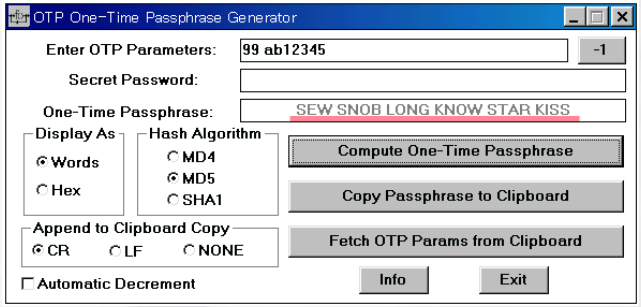
OTP Devices and Applications

Devices or applications that can generate one-time passwords

Can be classified into mathematical algorithm type, time-synchronized type and challenge type

More secure than using the traditional printed OTP card

OTP scratch card



OTP application

OTP device

Product Features

How APG82 PINhandy works

Using two-factor authentication

1. Cardholder inserts the EMV payment card (something you have) in the APG82 PINhandy
2. Enters PIN (something you know) using the device keyboard
3. A dynamic one-time password is generated and showed on the APG82 PINhandy display.
4. Cardholder can then use this password to perform secure online transactions, telephone orders or e-banking logons.

Product Features

- Operates in unconnected mode
- 10 numeric + 4 function keys
- High-contrast, 2 rows x 16 chars LCD
- Uses 2 AAA batteries
- Read and write all microprocessor cards with T=0 and T=1 protocols
- Supports 1.8V, 3V and 5V MCU and EMV cards
- Manage OTP, challenge-response and transaction data signing
- Tamper-evident seal to indicate unauthorized instruction
- Compact and handheld size
- Light & portable – approx. 1/5 of the weight of a can of soda (with batteries: 60g)

Compliance & Certification

Card Authentication Program (CAP)

Dynamic Passcode Authentication Program (DPA)

EMV Level1

RoHS Compliant

About MasterCard CAP

In September of 2002, MasterCard announced MasterCard SecureCode™ to offer flexible, robust, and easy to implement solutions for Cardholder Authentication for electronic commerce and other alternative channels. SecureCode allows for several different Cardholder Authentication Methods.

MasterCard's Chip Authentication Program (CAP) is one such cardholder authentication method.

MasterCard Components

1. Cardholder

2. Smart Card which supports CAP

E.g. M/Chip Select 2.05, M/Chip Lite 2.1, M/Chip 4 (Lite and Select)

3. Personal Card Reader (PCR)

Functions: (1) Interface to Cardholder

(2) Interface to Smart Card

4. CAP Token Validation Service (CTVS)

Functions: CAP token validation

Cardholder

PCR

CTVS

About VISA DPA

Visa has entered into a license agreement with MasterCard to allow the use of the Chip Authentication Programme (CAP) specification by Visa Members with Visa branded products.

Product Value

What are the Key Benefits of APG82?

Certified with Intl' standard *(Mastercard CAP and VISA DPA)*

Generate dynamic passwords

No need to remember dozens of passwords

Highly portable *(can be used anytime, anywhere!)*

Highly secure

(Unconnected mode → Impossible for hackers to steal the sensitive information in the card

Even if APG82 falls into the wrong hands, cannot be used if smart card is missing or if PIN is not known)

Area reserved for instructions/company logo printing

What are the Key Benefits of APG82?

Minimize cost of specialized programming like software drivers

Platform independent *(it's a standalone device!)*

Simple product ,relative low Technical Support Cost *(No drivers, no software enquiries /problems!)*

Avoid cardholders from leaving their cards behind *(allowed only semi-insertion of cards)*

Product Application

In what areas can we apply APG82?

PC/Network Security

eCommerce

E- Banking

How to Use APG82 - Overview

Sample Scenario: Electronic Audit

To ensure security, hash functions are applied in every data transmission process.

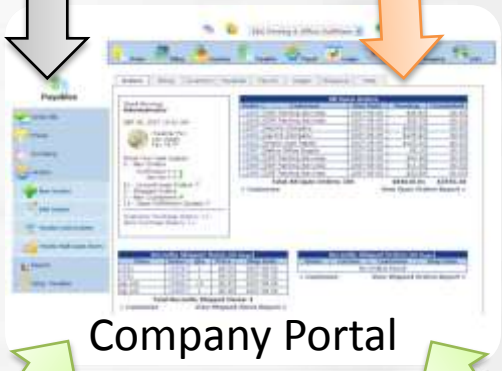
Backend Server

Login: Admin_U
PIN:
UpMan396453

Admin Terminal

996943

ADMIN: Retrieve financial statements to review and process



Company Portal

7:00 AM London

AUDITOR A: Submits audited financial statements

197328

Login: Aud_A
PIN:
Apass197328

Login: Aud_B
PIN:
xypqr284852

8:00 PM Berlin

AUDITOR B: Retrieve financial statements to be audited

284852

Thank You!!!

More information on:

http://www.acs.com.hk/apg82.php