Advanced Card Systems Ltd.
Card & Reader Technologies

APG8202

PINhandy OTP Generator

A Product Presentation




www.acs.com.hk

Presentation Rundown

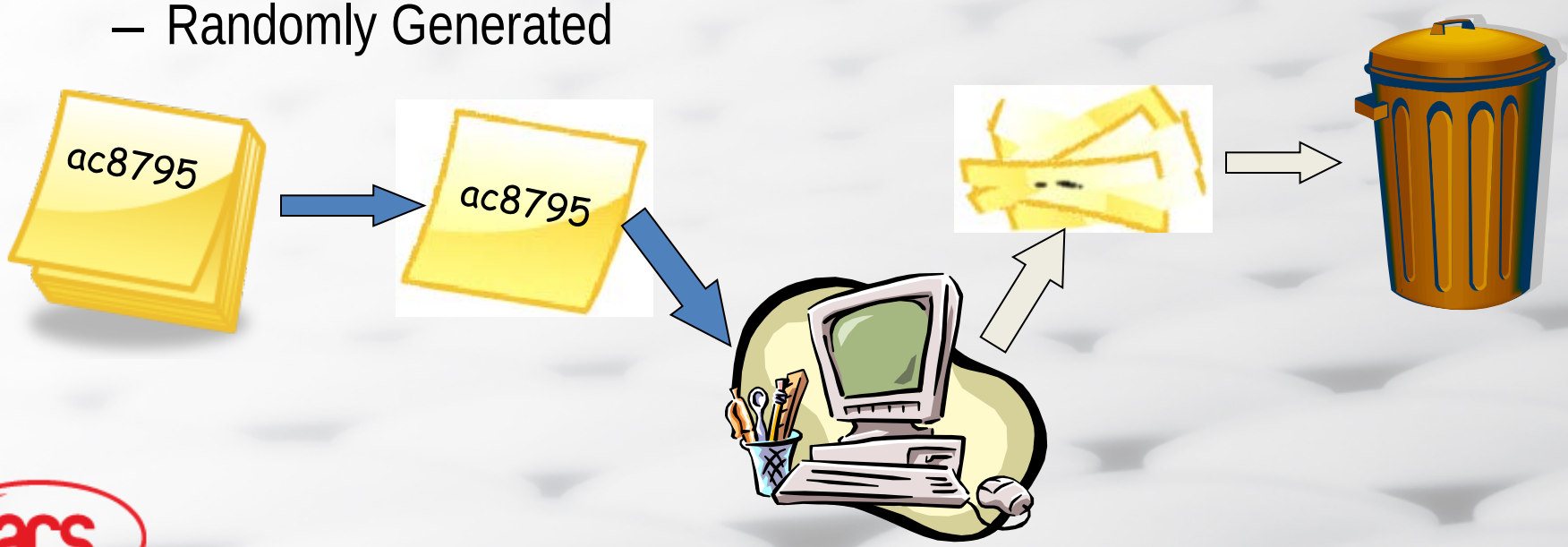
- Introduction
- Product Overview
- Product Features
- Product Value
- Product Applications
- Question and Answer

Introduction

- As technology becomes more and more sophisticated, fraud-related incidents in the banking sector also become more prevalent.
- These occurrences generate billions of dollars worth of losses and bring distress among credit and debit cardholders. Because of these, certain security measures and systems are created.
- In this regard, the APG8202 PINhandy OTP generator is a reliable tool that can be utilized to fight these occurrences.

Introduction: One Time Password

- One Time Passwords are password that can be used only ONCE
- Types of OTPs:
  - Predefined from a list
  - Randomly Generated



Introduction: One Time Password

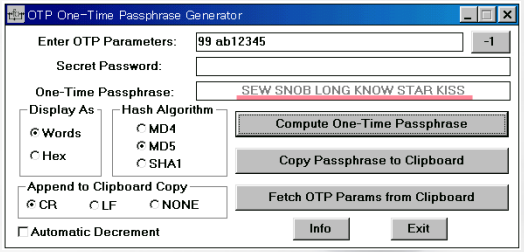
- More secure since its almost impossible to hack or phish.
- No need to remember multiple passwords for different systems.
- Dynamic passwords: Unique Password for Each Person

PIN	VS	OTP
Static Password		Dynamic Password
Memorization of multiple passwords		Little Memorization or no Memorization at all
Set of passwords is personalized		Two people will never have the same set of passwords

Introduction: OTP Devices

- 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 traditional printed OTP list

OTP scratch card



OTP applications

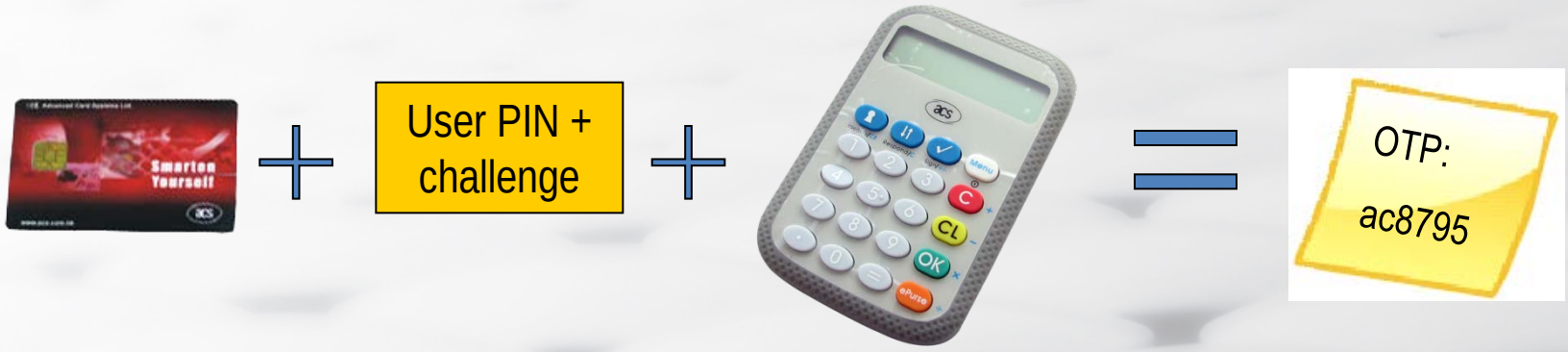
OTP devices

Product Overview

- OTP Generator
- Standalone Mode
- Supports PC/SC 2.01 Secure PIN Entry
- Handheld Device with Compact and Portable Design

Product Overview

- Supports Challenge-response and Transaction Data Signing Modes
- Requires the presence of smart card, PIN and challenge code prior the generation of OTP



Product Overview

Card Slot
(contact type connector)
(min 100K insertion cycles)

LCD *(2 x 16 chars)**

Large area for logo

CAP Authentication modes (L-R)
1. OTP
2. Challenge-response
3. Signature
4. TDS

20 Numeric Keys
(R: Reserved for Future Use)

Value-added
Calculator + E-purse
Function

*Graphical LCD for showing Logo
Multiple Languages: Simplified Chinese, Traditional Chinese, French, English

Product Overview

2 x CR2032 batteries
(5 years life expectancy)

Buzzer

Reset Button

USB port
(for APG8201only)

Product Features

Standalone Mode

Other Features:
Graphical LCD (128x24 Pixels)
Keypad with 20 Silicon Keys
Monotone Buzzer
Calculator Function

Size:
95mm x 60mm x 11mm

Contact Card Support:
ISO 7816 (Class A)
MCU Cards (T=0, T=1)

Supported Languages:
English
French
Traditional Chinese
Simplified Chinese

Product Features

ISO 7816 Support

EMV Level 1 Certified

Mastercard CAP

Mastercard PLA/AA4C

VISA DPA

UK APACS

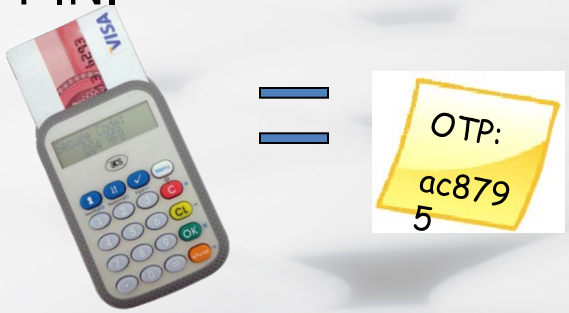
APG8202

CE and FCC Compliant

RoHS Compliant

Product Value

- It is specially designed to safeguard users from the emerging fraud attacks like Card-not-Present (CNP) fraud and emerging Man-in-the-Middle attacks.
- Key generated will be based on the smart card to be used with the device
- It provides proof that a card is present during an OTP process.
- The PIN is securely entered on the device rather than the vulnerable PC or workstation, hence eliminating the possibility of a Virus/Trojan getting hold of the PIN.



Application Overview

Windows Logon

Corporate Security

Online Gaming

eCommerce/eBanking

Loyalty System

Home Banking

e-Banking: Identify Mode

User browses the Online webpage of the online-banking, and try to logon, which username.

Insert the card
Choose Identify Mode
Input the PIN

OTP Token Generated:
4356 7869

Input Details Indicated in the Website (i.e. Card Number)
Input OTP generated in the website

Information Verified By the CAP/AA4C Backend Server

Once verified by the backend server the website will permit the transaction to continue

User can access his/her information online

e-Commerce: Challenge-Respond Mode

User browses the Online webpage to purchase goods/services

Merchant Website provides a challenge (i.e. random/hashed number)

Insert the card
Choose Mode 2
Input the PIN
Input Challenge

OTP Token Generated:
4356 7869

Input Details Indicated in the Website (i.e. Card Number)
Input OTP generated

Information Verified By the CAP/AA4C Backend Server

Once verified by the backend server the website will permit the transaction to continue

User is able to purchase goods and services

e-Banking: Sign Mode

User chooses to perform Fund Transfer

The e-Banking Website asks the user to sign the transaction to continue

Insert the card
Choose Mode 3
Input the PIN
Input Challenge
Enter Transaction Amount

OTP Token Generated:
4356 7869

Input Details Indicated in the Website
Input OTP generated

Information Verified By the CAP/AA4C Backend Server

Once verified by the backend server the website will permit the transaction to continue

User has successfully performed fund transfer

e-Banking: Transaction Data Signing

User chooses to perform Fund Transfer (large sums of money involved)

The e-Banking Website asks the user to verify the account number and sign the transaction to continue

Insert the card
Choose Mode 4
Input the PIN
Input Challenge
Input Account Number
Enter Transaction Amount

OTP Token Generated:
4356 7869

Input Details Indicated in the Website
Input OTP generated

Information Verified By the CAP/AA4C Backend Server

Once verified by the backend server the website will permit the transaction to continue

User has successfully performed fund transfer

Thank You!!!

More information on:

http://acs.com.hk/index.php?pid=product&id=APG8202

http://www.apg8202.com