Advanced Card Systems Ltd.
Card & Reader Technologies

APG8205

OTP Generator

A Product Presentation

www.acs.com.hk

Rundown

1. Introduction
2. Product Overview
3. Product Feature
4. Product Value
5. Product Application

Introduction

Introduction

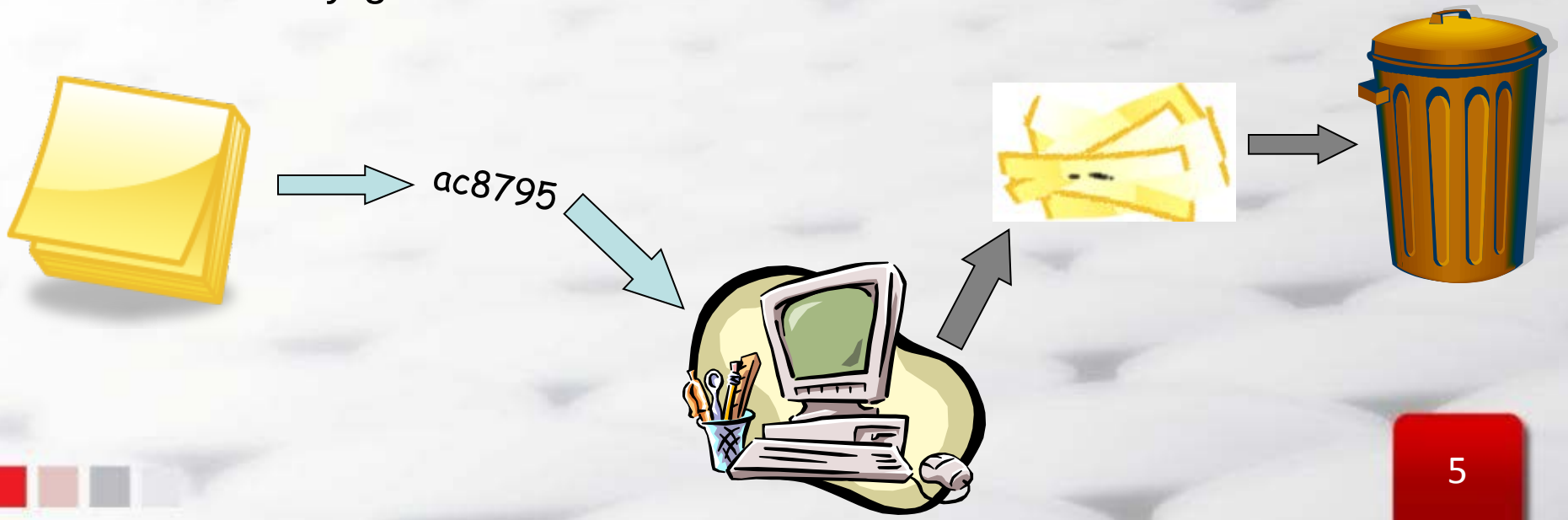
• As technology becomes more and more sophisticated, fraud-related incidents in the banking sector also become more prevalent.

• 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 APG8205 OTP generator is a reliable tool that can be utilized to fight these occurrences.

Introduction: One Time Password

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



Introduction: One Time Password

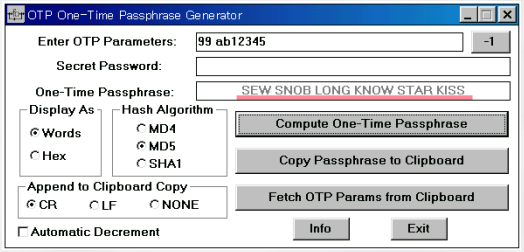
- More secure since its almost impossible to hack or phish.
- No need to remember multiple passwords for different systems.
- Dynamic passwords: Unique password for each person

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

Product Overview

APG8205 OTP Generator

- OTP Generator
- Standalone Mode
- Handheld Device with Compact and Sleek 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 Features

What are the Key Features of APG8205?

Large area for logo

CAP Authentication modes (L-R)

1. OTP
2. Challenge-response
3. Signature
4. TDS

Numeric Keys

LCD *(2 x 16 chars)**

Function Keys

Card Slot
(contact type connector)

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

What are the Key Features of APG8205?

Standalone Mode

Compact and Sleek Design
85.0 x 58.0 x 5.1 mm

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

Supported Languages
English
French

Certifications/Compliance
ISO 7816
EMV Level 1
MasterCard CAP
Visa DPA
CE, FCC, RoHS

Other Features:
Graphical LCD
Monotone Buzzer
Durable Tactile Keypad
Membrane with 20 Keys

Product Value

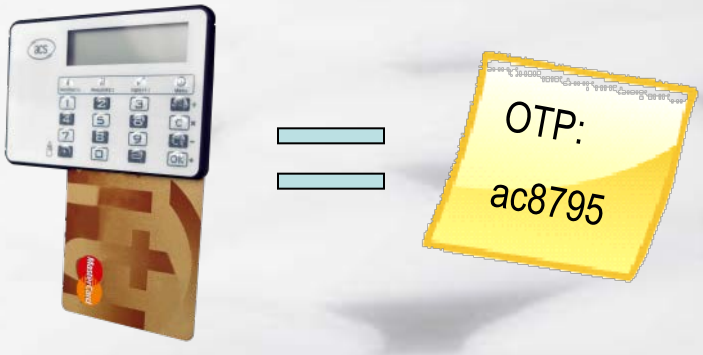
What are the Key Benefits of APG8205?

- 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.



Product Application

In what areas can we apply APG8205?

Windows Logon

Corporate Security

Online Gaming

e-Commerce/e-Banking

Loyalty System

Home Banking

How to Use APG8205?

e-Banking: Identify Mode

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

1. Insert the card.
2. Choose Identify Mode.
3. Input the PIN.

OTP Token Generated:
4356 7869

1. Input details indicated in the website (i.e., Card Number).
2. Input OTP generated in the website.

Information verified by the CAP/DPA backend server

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

User can access his/her information online.

How to Use APG8205?

e-Banking: Challenge-Respond Mode

User browses the online webpage to purchase: goods/services

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

1. Insert the card.
2. Choose Mode 2.
3. Input the PIN.
4. Input Challenge.

OTP Token Generated: 4356 7869

1. Input details indicated in the website (i.e., Card Number) .
2. Input OTP generated.

Information verified by the CAP/DPA backend server.

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

User is able to purchase goods and services.

How to Use APG8205?

e-Banking: Sign Mode

User chooses to perform Fund Transfer.

The e-Banking website asks the user to sign the transaction to continue.

1. Insert the card.
2. Choose Mode 3.
3. Input the PIN.
4. Input Challenge.
5. Enter Transaction Amount.

OTP Token Generated:
4356 7869

1. Input details indicated in the website.
2. Input OTP generated.

Information verified by the CAP/DPA backend server.

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

User has successfully performed fund transfer.

How to Use APG8205?

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.

1. Insert the card.
2. Choose Mode 4.
3. Input the PIN.
4. Input Challenge.
5. Input Account Number.
6. Enter Transaction Amount.

OTP Token Generated:
4356 7869

1. Input details indicated in the website.
2. Input OTP generated.

Information verified by the CAP/DPA backend server.

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

User has successfully performed fund transfer.

Thank You!