MF-WEB05A

USER MANUAL

TCP/IP ETHERNET

HTTP WEB CLIENT

RFID TERMINAL

8th January, 2014

AVEA International Company Limited

(http://avea.cc)

Table of Contents

Table of Contents 1

MF-WEB05A TCP/IP Ethernet HTTP Web Client RFID Terminal 3

1. SETUP THE READER 4

1.1 AVAILABLE SETTINGS 4

1.2 DHCP MODE 5

1.3 SUPPORTED CARD TYPE 5

2. INSTALLATION 6

2.1 POWER REQUIREMENTS 7

2.1.1 Terminal Block 7

2.1.2 Power from Cat-5/e Ethernet cable 7

2.2 EXTERNAL RELAY CONTROL 7

2.3 CONTACT SWITCH 8

2.4 BATTERY 8

2.5 MECHANICAL DIMENSIONS 8

3. SOFTWARE 9

3.1 REQUESTS TO HTTP SERVER 9

3.1.1 \avea.php 9

3.1.2 $date and $time 9

3.1.3 $id 9

3.1.4 $code 10

3.1.5 $pin 10

3.1.6 $cmd 10

3.1.7 $deviceid 11

3.1.8 $mode 11

3.1.9 $ver 11

3.1.10 $contact 11

3.1.11 $sid 11

3.1.12 $ulen 11

3.1.13 $uid 12

3.1.14 $md5 12

3.1.15 $data 12

3.2 RESPONSES FROM HTTP SERVER 13

3.2.1 HB=xxxx 13

3.2.2 BEEP=x 13

3.2.3 CK=YYYY-MM-DD HH:MM:SS 13

3.2.4 GRNT=xx *14*
3.2.5 DENY *14*
3.2.6 MSG=xxxxxxxx *14*
3.2.7 ACPIN=xxxx *15*
3.2.8 CLEAR=ALL *15*
3.2.9 AC=xxxxxxxxxx *15*
3.2.10 DC=xxxxxxxxxx *15*
3.2.11 ROOT=xxxxxxxx *15*
3.2.12 SHOWPIN=x *16*
3.2.13 EXT=x *16*
3.2.14 DHCP=x *16*
3.2.15 IP=xxx.xxx.xxx.xxx *17*
3.2.16 GW=xxx.xxx.xxx.xxx *17*
3.2.17 NM=xxx.xxx.xxx.xxx *17*
3.2.18 WS=xxx.xxx.xxx.xxx *17*
3.2.19 PT=xxxxx *18*
3.2.20 RLY=x *18*
3.2.21 SID=xxxxxxxx *18*
3.2.22 MD5=xxxxxxxxxxxxxxxx *18*
3.2.23 MKEY=Nxxxxxxxxxxxx *18*
3.2.24 MREAD=Nxx *19*
3.2.25 MAUTH=x *19*

4. PHP CODE EXAMPLE 20

MF-WEB05A TCP/IP Ethernet HTTP Web Client RFID Terminal

MF-WEB05A is a TCP/IP Ethernet based RFID terminal for reading MIFARE type RFID cards. It is implemented as a standalone HTTP web client (i.e. no extra computer is needed).

Upon RFID card detected by the reader, it will sent a GET request to the web server and requesting the page \avea.php. The server responses with standard HTTP reply to reader with embedded controls between <AVEA> and </AVEA> tags.

Various page extension are selectable, like .php, .asp, .cfm, .pl, .htm, .html and .aspx. So various HTTP web server systems (e.g. IIS and ASP from Microsoft; Apache with PHP with MySQL database server from Unix/Linux; standard html web server) can be used.

Since the system is a standard web based system, no programming is required. Just a simple design of a web page, a complete and powerful access control system and time attendance system can easily be implemented.

1. Setup the reader

In order to work properly, MF-WEB05A must be configured correctly.

To enter configuration mode: hold the ‘*’ key while applying the power to the reader. ‘CONF’ will be shown on the reader.

Press ‘*’ to cycle the parameters to be configured.

Press '#' to store the changed or '*' to cancel.

1.1 Available Settings

Parameter	Description	Default
IP	IP address of the reader itself	192.168.1.234
Gate	Gateway IP address	192.168.1.1
Net	Netmask	255.255.255.0
Ser	HTTP server IP address	192.168.1.1
Port	HTTP server port number	80
Ext	Page extension	php
DHCP	DHCP protocol enable	no

- to edit the parameter, press ‘#’ key.
- ‘.’ Is entered by pressing ‘#’ key, i.e. to enter 192.168.1.123, the key sequence is 192#168#1#123,
- then press ‘#’ key to confirm entry
- or ‘*’ key to cancel the operation.
- to set the Ext, press any numeric key to cycle the available options (.php, .asp, .cfm, .pl, .htm, .html and .aspx).
- to toggle the DHCP option, press any numeric key.

1.2 DHCP mode

When DHCP is enabled, automatic configuration of the MF-WEB05A can be done by an external DHCP server. The DHCP server may be configured to response the options www-server, i.e. option 72. If setted, the server IP address will be configurated.

Example of dhcpd.conf of a LINUX system:

```
#example of dhcpd.conf
ddns-update-style    ad-hoc;

subnet 192.168.1.0 netmask 255.255.255.0 {
     # --- default gateway
     option routers 192.168.1.1; # default gateway
     option subnet-mask 255.255.255.0;   # netmask
     option www-server 192.168.1.123;    # it may be setup to the web server’s IP
     range dynamic-bootp 192.168.1.10 192.168.1.99;
     default-lease-time 300;
     max-lease-time 3600;
 }
```

1.3 Supported Card Type

The reader is supported to readout the UID of the following card type:

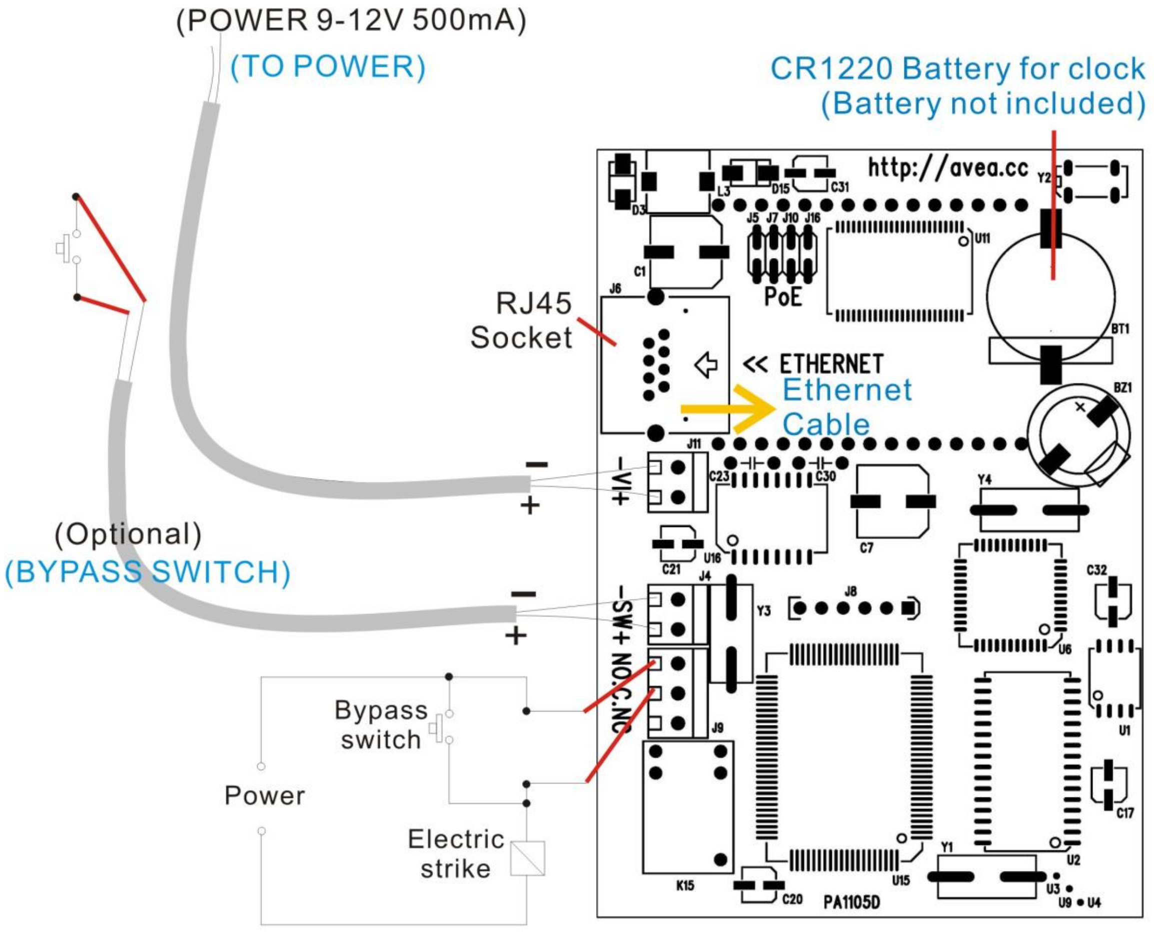
- Mifare1 S50/S70
- Mifare Ultralight
- Mifare Pro
- Mifare DESFire
- Mifare Plus
- Mifare derivatives

For reading the contents using KEYA or KEYB, only S50/70 is supported.

2. Installation

In order to work properly, MF-WEB05A must have stable power supply, a 10-baseT Ethernet connection, and an optional electric strike or magnetic lock.

Make sure to power off the power supply unit before any wirings change. Otherwise, it will cause permanent damage to the reader.



Remarks:

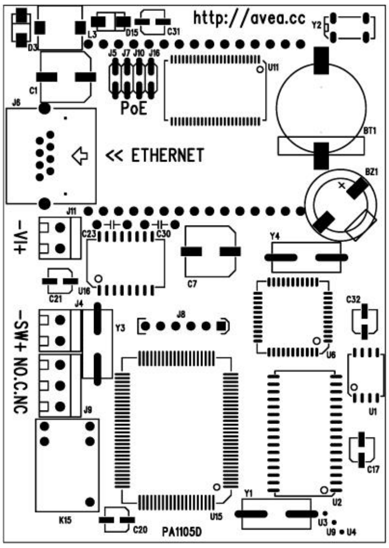
1. Connection to the electric strike.
2. Connection to an internal bypass switch.
3. Connection to Ethernet network.
4. Connection to power supply for MF-WEB05A.

2.1 Power Requirements

MF-WEB05A requires 9 to 12V DC 500mA for normal operation. There are two ways to supply the power to the reader:

2.1.1 Terminal Block

Apply the power supply to the terminal block J11, with positive terminal to VI+ and negative terminal to VI- (ground). The voltage can be 9V to 12V and the minimum current rating is 500mA or bigger.



2.1.2 Power from Cat-5/e Ethernet cable

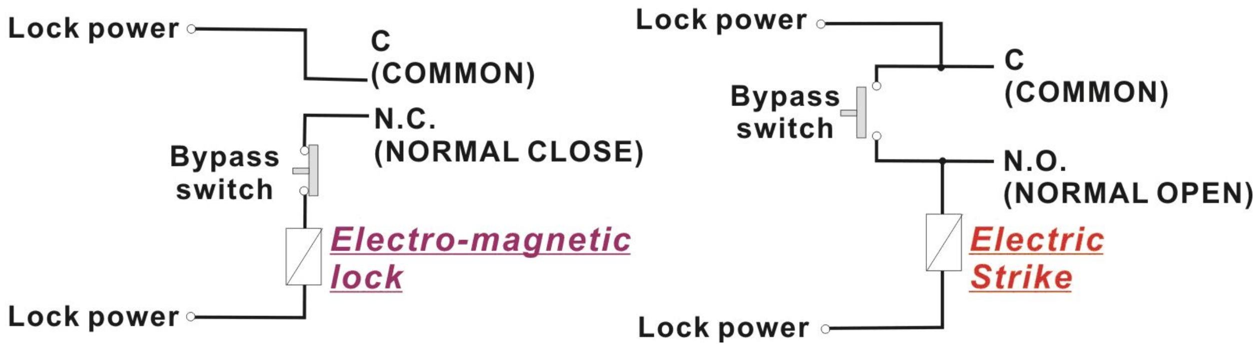
Besides the supply power through J11, the power can go through the Ethernet cable on the RJ45 connector, where Pin 7 and 8 is connected to VI- (ground), and Pin 4 and 5 is connected to VI+. Meanwhile, jump block PoE must be shorted out by four two-pin jumper headers.

2.2 External Relay Control

MF-WEB05A is built-in with a user controllable relay output on the terminal block J9, where:

NC - normal close, it is connected to C normally.
C - common, it will connects to either NO or NC, but not both.
NO - normal open, it is open circuit normally.

The maximum switching voltage of the relay is 120VAC or 60VDC, and the maximum switching current is 2A.It can be used to connect to the bypass switch of an electric strike for door access controlling. Overloading the maximum ratings may cause damages to the reader permanently and cannot be repaired anymore.



2.3 Contact Switch

MF-WEB05A allows a external contact switch (i.e. a push button) to be connected to the -SW+ terminals. The changes of its status (i.e. shorted or opened), will post corresponding messages to the web server.

2.4 Battery

A CR1220 type lithium battery is required to maintain the operation of the real-time clock running properly during power down. If it is not installed, the clock will reset every time after power removed.

2.5 Mechanical Dimensions

Height:	100mm
Width:	71mm
Depth:	30mm

3. Software

MF-WEB05A is a HTTP client with PHP enabled. It will send PHP URL requests to the HTTP server with the various parameters. And it accepts responses from the HTTP server to perform various actions on the reader. The manual is based on using PHP version 4. It may have some differences across various versions.

3.1 Requests to HTTP server

The followings are the variables presented to the PHP. User can access it correspondingly.

3.1.1 \avea.php

The reader send a GET request to access a fixed web page of the HTTP server: avea.php located on the root of the website. The file extension is user selectable, e.g. avea.asp, avea.cfm avea.pl, avea.htm and avea.html. But it is server changeable to any numeric filename located on the root.

3.1.2 $date and $time

Hold the date and time of that request. The format of date is YYYY-MM-DD, e.g. 2007-01-23 means 23rd Jan 2007. The format of time is HH:MM:SS where HH is hour, MM is minute and SS is second.

3.1.3 $id

It is the IP address of the reader, e.g. 192.168.1.234. It must be set to different value for each reader in order to function properly.

3.1.4 $code

It is the truncated UID (lower 3 bytes only) of the ID card presented to the reader.

3.1.5 $pin

It is the PIN number entered by the user and terminated by the '#' key. The maximum length is 8-digit number.

3.1.6 $cmd

It holds the action that was taken on the reader.

I. $cmd=PU, it is sent once after the reader is just power up.

II. $cmd=CO, it is sent with an ID card is read on the reader. The card number is stored in $code.

III. $cmd=PO, it is sent when a PIN number is entered and terminated with '#' key. The PIN number is stored in $pin.

IV. $cmd=CP, it is sent when PIN number is entered and terminated with ID card read. The card number is stored in $code and the PIN number is stored in $pin.

V. $cmd=TS, it is sent when '*' key or '#' key is pressed on the reader.

VI. $cmd=HB, it is sent when the programmed heartbeat rate is reach. The default heartbeat rate is 300 seconds.

VII. $cmd=SW, it is sent once when contact switch is just shorted or opened.

VIII. $cmd=PG, it is sent when the reader is being pinged.

3.1.7 $deviceid

This is the 32-bit unique ID of the reader.

3.1.8 $mode

For internal use, $mode indicates the operating mode.

3.1.9 $ver

For internal use, $ver indicates the software version.

3.1.10 $contact

It is used with $cmd=SW to indicate the state of the contact switch. If the switch is opened, $contact=OPEN. If the switch is closed, $contact=CLOSE.

3.1.11 $sid

This is the value set by the SID response. It is permanently stored until next change by the user.

3.1.12 $ulen

It is the byte length of the UID of the MIFARE card. It can be 4, 7 or 10.

3.1.13 $uid

It is the UID of the MIFARE card, the string is in hexadecimal format and is of variable size. $ulen tells the length.

For examples:

for $ulen=4, $uid=9E80732F
for $ulen=7, $uid=8877665E03441A
for $ulen=10, $uid=123456789ABCDEF01234

3.1.14 $md5

It is the MD5 checksum of the user's MD5 secret key, date and time. It will be sent together in the request for identification purpose.

For examples:

assuming
- MD5 secret key is '01234567' (ASCII),
- date of the request is '2012/08/08' (ASCII),
- time of the request is '10:19:54' (ASCII)

the combined string is
- '012345672012/08/08-10:19:54' (ASCII)

hence the MD5 checksum of the combined string is
- b62a8cf4adfdd10874f1121686b0bba9

On the server side, the MD5 secret key is known, so it can compute the MD5 checksum and check against the received checksum for verification.

Since the MD5 secret key is unknown to others, only those authenticated reader can sent out correct MD5 checksum.

3.1.15 $data

This is the data of the block readout in 32 digit hexadecimal values.

3.2 Responses from HTTP server

After sending request, MF-WEB05A will wait for a response from the HTTP server. It looks for the starting flag <AVEA> and the ending flag </AVEA>. Then it interprets the strings in between. There must be no space between the keywords and parameters. The maximum size of the response packet should be less than 1024 bytes.

The following responses are supported:

3.2.1 HB=xxxx

Set the heartbeat rate of the reader in seconds. It is a fixed length format in decimal value. Example:

HB=0300 set the reader send a heartbeat request to the HTTP server once in 300 seconds.
HB=0000 to disable the heartbeat request.

3.2.2 BEEP=x

Make a beep sound on the reader. It is a fixed length format. Example:

BEEP=1 make a short beep.
BEEP=0 make a long beep.

3.2.3 CK=YYYY-MM-DD HH:MM:SS

Set the clock of the reader. The year must be in 2000 to 2099. It is a fixed length format. Example:

CK=2007-01-23 12:34:56 set the clock to 23rd Jan 2007, pm12:34:56.

3.2.4 GRNT=xx

Set the reader to a grant access state, i.e. to engage the relay from NO state to NC state for xx seconds and return to NO state. It is a fixed length format. Example:

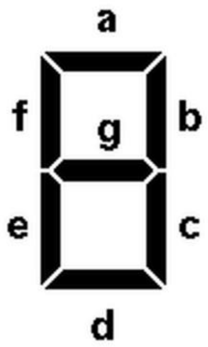
GRNT=03 set the relay to NC state for three seconds and return to NO state.

3.2.5 DENY

Set the reader to a deny access state, i.e. to make sure the relay is in NO state.

3.2.6 MSG=xxxxxxxx

Display a 4-digit message on the LCD display of the reader. It is a fixed length format.
The message is a bitmap pattern to the 7-segment LCD digit. Each two hexadecimal number represents a LCD digit. The leftmost digits represent the leftmost LCD digit.



The mapping is as follows:

0x01 will turn on the segment a
0x02 will turn on the segment b
0x04 will turn on the segment c
0x08 will turn on the segment d
0x10 will turn on the segment e
0x20 will turn on the segment f
0x40 will turn on the segment g

By adding the values together, multiple segments can be displayed at the same time. Example:

MSG=3f737937 to display ‘OPEN’ on the LCD.

3.2.7 ACPIN=xxxx

Set a 4-digit access PIN into the reader. In any situation, press “#” and the access PIN will allow granted access to the relay. If the access PIN number is ‘0000’, no access will be granted at all. It is a fixed length format.

3.2.8 CLEAR=ALL

The reader will clear the offline access right table, i.e. no offline access will be granted to any card.

3.2.9 AC=xxxxxxxxxx

The reader will store the offline access right for the specific card number (10-digit), i.e. press ‘#’ and swipe the card over the reader will grant offline access to that card. It is a fixed length format. Only lower 3 bytes of the UID is used. A maximum of 200 cards can be stored for offline access.

3.2.10 DC=xxxxxxxxxx

The reader will remove the offline access right of the specific card number (10-digit). It is a fixed length format.

3.2.11 ROOT=xxxxxxxx

This will change the root page to be access by the reader. It is a fixed length format. For example: ROOT=00024689, this will make the reader to access the page /24689.php rather than the default /avea.php. By setting ROOT=00000000 will reset to access the default page.

3.2.12 SHOWPIN=x

This will affect whether the pin number is shown on the LCD display during entering. If SHOWPIN=1, the pin number will be shown. If SHOWPIN=0, the pin number will be hidden.

3.2.13 EXT=x

This will change the root page’s file extension to be access by the reader. It is a fixed length format.

Value of x	File extension
0	.php
1	.asp
2	.cfm
3	.pl
4	.htm
5	.html
6	.aspx

3.2.14 DHCP=x

This will control DHCP feature of the reader. If DHCP=1, DHCP is enabled. If DHCP=0, DHCP is disabled. If enabled, it will send requests to DHCP server to acquire the following items:

- host IP
- netmask
- default gateway
- www-server IP

3.2.15 IP=xxx.xxx.xxx.xxx

This is a fixed length command and values are in decimal. It will change the IP address of the reader. Example:

IP=192.168.001.234

3.2.16 GW=xxx.xxx.xxx.xxx

This is a fixed length command and values are in decimal. It will change the default router of the reader. Example:

GW=192.168.001.002

3.2.17 NM=xxx.xxx.xxx.xxx

This is a fixed length command and values are in decimal. It will change the netmask of the reader. Example:

NM=255.255.255.000

3.2.18 WS=xxx.xxx.xxx.xxx

This is a fixed length command and values are in decimal. It will change the web server IP address to be accessed by the reader. Example:

WS=192.168.001.001

3.2.19 PT=xxxxx

This is a fixed length command and values are in decimal. It will change the port number to be used to access the web server in decimal. Example:

PT=00080

3.2.20 RLY=x

This is a fixed length command and values are in decimal. If RLY=1, the relay will be turned on. If RLY=0, the relay will be turned off. The state of relay will be affected by the subsequence commands.

3.2.21 SID=xxxxxxxx

This is a fixed length command and values are in hexadecimal value. It is a non-volatile value and will not changed after power removed.

3.2.22 MD5=xxxxxxxxxxxxxxxx

This is a fixed length command and 64-bit values are in hexadecimal value. It is a non-volatile value and will not changed after power removed. This is the secret key used for computing MD5 checksum.

3.2.23 MKEY=Nxxxxxxxxxxxx

This is a fixed length command and values are in hexadecimal value. It is a non-volatile value and will not changed after power removed.

N is either ‘A’ or ‘B’ to specify which key to be set.
xxxxxxxxxxxx is the value of the key in 12 hexadecimal digits.
e.g. MKEY=ADC1234567890 will set KEYA to value DC1234567890 (hex).

It is not recommend to transmitting the key over public network instead set it in a safe and private network environment.

3.2.24 MREAD=Nxx

This is a fixed length command and values are in hexadecimal value. It is a non-volatile value and will not changed after power removed.

N is either ‘A’ or ‘B’ to specify which key to be set.
xx is the block number to be read in hex.
e.g. MREAD=B0C will set the reader to read block number 12 (decimal) using KEYB.

3.2.25 MAUTH=x

This is a fixed length command, where x is the value authorization mode. It is a non-volatile value and will not changed after power removed.

MAUTH=0 will not read any block of data, i.e. authentication is disabled.

MAUTH=1 will read block of data using the key specified by MREAD. If authentication is success, the data block will be sent to the server as well as the UID. If authentication is failed, only the UID will be sent to the server.

MAUTH=2 will read block of data using the key specified by MREAD. If authentication is success, the data block will be sent to the server as well as the UID. If authentication is failed, no request will be sent to the server.

4. PHP Code Example

The following is an self explainable example of PHP version 4 script located on the HTTP server. The filename is \avea.php.

```
<html>
<body>
<?php
$now=time();   // stamp the current time
$cmd=_GET[“cmd”]; // get the command from the reader
$date=_GET[“date”]; // get the date of card code is logged
$time=_GET[“time”]; // get the time of card code is logged
$st=date('Y-m-d H:i:s',$now); // set the datetime string to  correct format
$mycard=359452;     // replaced by your card number
$mypin=1234;        // replaced by your PIN number
$rtime=$date . $time;    // access the date and time of the reader

echo "<AVEA>"; // starting flag
switch ($cmd) {
case "PU":     // power up
     echo "CK=$st"; // set clock
     break;
case "CO":     // card only
     $code=_GET[“uid”]; // get the card code
     if ($code==$mycard) {
          echo "MSG=3f737937"; // show message OPEN
          echo "GRNT=01";     // grant access
     } else {
          echo "DENY";   // deny access
     }
     break;
case "PO":     // pin only
     $pin=_GET[“pin”]; // get the PIN
     if ($pin==$mypin) {
          echo "MSG=3f737937"; // show message OPEN
          echo "GRNT=01";     // grant access
     } else {
          echo "DENY";   // deny access
     }
```

```
          break;
     case "CP":     // card + pin
          $pin=_GET[“pin”]; // get the PIN
          $code=_GET[“uid”]; // get the card code
          if (($code==$mycard) && ($pin==$mypin)) {
               echo "MSG=3f737937"; // show message OPEN
               echo "GRNT=01";     // grant access
          } else {
               echo "DENY";   // deny access
          }
          break;
     case "TS":     // * key
          echo "ACPIN=1234"; // add offline access PIN, i.e. press #1234 will be access granted
          echo "AC=0005793663"; // add offline access card, i.e. press # and swipe this card will be access
granted
          echo "DC=0005793664"; // remove offline access card, i.e. press # and swipe this card will be
not access granted
          echo "MSG=40763040"; // show message -HI-
          echo "BEEP=0"; // make long beep
          break;
     case "HB":     // heartbeat
          echo "CK=$st"; // set clock
          break;
     }
     echo "</AVEA>";     // ending flag
     ?>
     </body>
     </html>
```