SecurID Methods and Procedures
Michigan

SecurID Methods and Procedures
Table of Contents

SecurID Card Administration Methods and Procedures

Login Methods and Procedures

Attachments

SecurID Card Administration
Methods and Procedures

Purpose

To provide standards and procedures for users with dial-in access requirements to Ameritech corporate networks where SecurID card authentication technology is used with the SecurID security system.

Scope

This standard applies to Ameritech corporate computer systems and central office switches where SecurID card authentication is utilized to protect dial-in access to Ameritech corporate networks.

General Overview

The SecurID security system, utilizing SecurID cards for authentication is a security product designed to protect dial-in facilities to Ameritech corporate networks from unauthorized users. The system consists of two major elements: the SecurID card, developed by Security Dynamics and a security software running on either a mainframe or midrange computer. These two elements form a highly secured process for recognizing and recording attempted unauthorized entries into Ameritech corporate networks, while providing quick and easy access to authorized users.

The SecurID card is a sophisticated hand held authentication device and is used instead of a password. The card is the size of a credit card and convenient to carry. Each card is programmed with a unique seed number and proprietary algorithm. This information is also stored in the SecurID security system. The random display of numbers on the face of the card changes every sixty seconds. Small horizontal bars to the left of the display lets the user know, in 10 second increments, how long the number has been displayed. A SecurID card's life cycle is approximately three years. Some cards will have a shorter life cycle due to storage time or reuse.

The administration of the SecurID cards and the SecurID security system is handled by Ameritech -Distributed Security. Office hours and phone coverage for card requests and profile updates is provided between 8:00am - 5:00pm ET/CT, Monday through Friday. Dialup and login access problem support is available, 24 hours a day, 7 days a week, contact the appropriate SecurID Administration Center Hotline for the duty pager number. Address and telephone information:

Illinois and Wisconsin

Ameritech -Distributed Security
Attn: SecurID Administration
225 W. Randolph, Room HQ9A
Chicago, IL 60606
Hotline: 312-727-8923
FAX: 312-727-4259
E-Mail Acct: carroll,barb

Indiana, Michigan and Ohio

Ameritech -Distributed Security
Attn: SecurID Administration
23500 Northwestern Hwy., Room A220
Southfield, MI 48075
Hotline: 810-424-7505
FAX: 810-424-2550
E-Mail Acct: amrtch,secidadm-east

Client Help Centers:

Illinois & Wisconsin	312-930-3800
Indiana	317-265-5311
Ohio & Michigan	810-424-1111

SecurID Card Procurement

Distributed Security will control the acquisition, administration and distribution of SecurID cards for all users who are authorized to access any Ameritech computer system, corporate network, and/or central office switch. A *SecurID Card Request* form, AM860 *(Attachment A)*, must be properly completed to receive a SecurID card. Forms are provided by the SecurID Administrator and available through Forms Management.

An Ameritech employee must obtain the approval of their immediate Supervisor for all *replacement* card requests. Cost of card will be charged back to originating district.

A non-Ameritech user must have the approval of an approved Ameritech sponsor to obtain a card. Cost of card will be charged back to the Ameritech sponsor's district.

All request forms should be forwarded to the appropriate SecurID Administration Center as defined below.

Illinois and Wisconsin

Ameritech -Distributed Security
Attn: SecurID Administration
225 W. Randolph, Room HQ9A
Chicago, IL 60606
Hotline: 312-727-8923
FAX: 312-727-4259
E-Mail Acct: carroll,barb

Indiana, Michigan and Ohio

Ameritech -Distributed Security
Attn: SecurID Administration
23500 Northwestern Hwy., Room A220
Southfield, MI 48075
Hotline: 810-424-7505
FAX: 810-424-2550
E-Mail Acct: amrtch,secidadm-east

New User Requests

A *SecurID Card Request* form AM860, *(Attachment A)* must be completed with all required approvals to obtain a SecurID card and/or to obtain access to a application(s) on the corporate networks. After ALL required signatures have been obtained, the user or the Application Coordinator will forward the form to the SecurID Administrator for processing. If access to a requested destination is denied, the user will be notified.

All Non-Ameritech new user requests *must* have an Ameritech sponsor's dated approval signature in the *"Request Approval"* section to obtain a SecurID card.

All new user requests must specify if they will require a SecurID card for any period less than eighteen months in the *"Temporary User"* section. The user must document the card return date.

The SecurID Administrator will provide the SecurID card and a documentation package to the authorized user in two separate mailings. The new user should verify that they have received the following materials:

Documentation package:
- -SecurID Methods and Procedures
- -Login Information letter

SecurID Card package:
- -SecurID card with return label affixed
- -SecurID protective card holder
- -Care of SecurID card instructions

Contact the appropriate SecurID Adminstration Center immediately, if you are missing any of the above information.

New users that already have a SecurID card do not have to be issued another card. The requestor must provide the SecurID card serial number in the "Existing SecurID Card Holder" section. The User will receive in one mailing the following information:

- -Care of SecurID card Instructions
- -Methods and Procedures
- -Login Information

Users that currently use a group ID or a script file to access a host computer will be required to have an individual Login and SecurID card. Application Administrators and other authorized personnel can request a secondary SecurID card to allow vendor, one-time and emergency access.

Damaged/Defective or Lost/Stolen SecurID Cards

The user must IMMEDIATELY contact the appropriate SecurID Hotline when a SecurID card is lost or stolen. The SecurID Administrator will disable the card in the SecurID security system. The user will have to complete a new *SecurID Card Request* form and obtain their immediate Supervisor's dated signature to receive another SecurID card. The cost of the card will be charged bach to the originating district or the Ameritech sponsor's district. The User can access the Ameritech network by following the ***Emergency Access*** procedures while waiting for a replacement card.

Inactive Cards

The SecurID Administrator will review card usage to determine if a card should be disabled if inactive for a sixty day period. The user will be notified and asked to explain the non-usage. If the explanation is reasonable, it will be noted on the user's records and the SecurID card will remain active. Otherwise, the card will be disabled and the user will be asked to return the SecurID card.

Users that no longer require the SecurID card should complete a *SecurID Card Request* form and return the card and form to the SecurID Administrator at the address provided on the back of the card. If the User requires dial-in access after the card is returned, the ***New User Request*** procedures must be followed.

Expired SecurID cards

A SecurID card's life cycle is approximately three years. Some of the cards will have a shorter life cycle due to storage time or reuse. The expiration date is built in the card and at a certain date and time, the display goes blank and the card can not be used again.

The SecurID Administrator will notify the user 60 days before the expiration of the card. In addition the SecurID security system will broadcast a warning message for the user to see after every successful login authentication. Broadcast messages start 60 days before the card expiration date.

DO NOT THROW THE CARD AWAY!! Return the expired card to the appropriate SecurID Administration Center with a completed *SecurID Card Request* form.

Users that require another SecurID card, may do one of the following:

1. Complete a *SecurID Card Request* form (check box - reissue request)
2. Send an e-mail to the appropriate SecurID Adminstrator. Include your Login, card serial # and current mail address.

It is recommended that the User process the reissue request before the card expires. The cost of the card will be charged back to the originating district or the Ameritech sponsor's district.

Emergency Access

Emergency access provides one-time access to authorized SecurID users. To obtain emergency access, the user should contact the appropriate SecurID Hotline. In some instances, the SecurID Hotline will refer the user to a local Administrator for access.

The SecurID user who was issued the SecurID card, should be prepared to provide their name, Login and SecurID card serial number for authentication purposes. The Administrator providing the access will be responsible for logging the date and authentication information of each user to whom access is granted.

Temporary Access

Temporary access is for a user that requires a SecurID card for eighteen months or less. The user will need to follow the ***New User Request*** procedure and specify the length of time the access is needed. A user requiring an extension to a previously authorized request must complete a new *SecurID Card Request* form and obtain the appropriate approvals. The user is responsible for returning the card to the appropriate SecurID Adminstration Center at the expiration of the temporary access period.

Login Methods and Procedures

SecurID Card Initialization -Michigan Server

SecurID card initialization on the Michigan security server can only be done if you've requested access to an application/system protected by this system.

As soon as the user receives the SecurID card, they should notice whether or not the number displayed on the face of the card changes every 60 seconds. If not, the card is defective or damaged and should be returned to the SecurID Administrator.

Modem pools have been established in each state *(See **Attachment B** for listing)*. The users are responsible for understanding the nuances of their terminal or communication package setup. It is recommended that the user's dial-out modem have error correction/reliable mode/MNP enabled. The user's PC/terminal should be set to 8 databits/no parity/1 stopbit.

SecurID does not recommend users scripting their terminals for access into the SecurID security system in the event they have difficulty logging in unless they are creating the scripts themselves. Scripting a PC/terminal allows the user a short cut method for logging in, etc. by programming a function key or code. There are several reasons why a user might have difficulty logging in because of their User ID, passcode, dial-in modem pool, expired PIN, etc. If scripting is programmed, the user may not be sure what was set up and consequently it becomes difficult to assist them. In this case, the user should make sure their terminal is programmed for a manual method in the event of a problem. The user should contact their PC/terminal coordinator first for assistance on their data communication setup or the local Client Help Center (CHC) may be of assistance.

The new user must follow the steps described in ***Logging In For The First Time*** to establish a PIN for their card. This must be completed before an application or destination can be accessed for the first time.

USERID

The SecurID Administrator will establish a UserID for each user based on the Ameritech User Identification Standard, 16-350. The UserID will be assigned in "lower" case, the SecurID security system is "UPPER" and "lower" case specific.

PASSCODE

A passcode consists of a user created PIN and the digits currently displayed on the front of the SecurID card.

Users will create their own PIN when they a) login the first time, b) want to reset their PIN, c) the PIN expires, d) when the SecurID Administrator deems it necessary to put them in *New PIN mode*. Users can change their PIN after a minimum age period of 1 day. A previously used PIN can be reused.

Users that have forgotten their PIN must contact the appropriate SecurID Hotline.

PIN Format

- Must be four characters long and can be alpha and/or numeric
- Cannot have three or more characters in a simple sequence (i.e. aaaa, 1111, 1234, 4321, 3690, 0963, aceg, geca)
- The PIN is UPPER and lower case specific. It is very important that the user does not have "Caps Lock" activated if their PIN does not include UPPER case character(s).

Expired PIN Format

A new PIN must differ from the expired PIN in at least three character positions. Another restriction is that the new PIN cannot be a circular shift of the expired PIN or its reverse (i.e. Expired PIN = junk. New PIN cannot be unkj, nkju, knuj, etc.)

PIN Expiration

A PIN will expire after the maximum age of 180 days. When the PIN expires, the SecurID security system will prompt the user to change their PIN during the login process.

PIN Reset

If the user forgets their PIN, they must call the appropriate SecurID Hotline to have the PIN reset. The user will be prompted to establish a new PIN during the next login sequence.

Login Attempts

Users will have three attempts in one session to pass authentication from the SecurID security system. Users that cannot be authenticated by three attempts will be disconnected from their session.

A user who is unsuccessful in logging in after three successive sessions (9 attempts) will be disabled in the SecurID security system because an unauthorized access attempt is suspected. A legitimate user who becomes disabled may call the appropriate SecurID Hotline for assistance. The user will only be "enabled" after providing sufficient authentication information.

Logging In For The First Time

1. Dial-in to one of the ***Michigan Security Server*** modem pools. *(See Attachment B)*
   - System response: *"UserID:"*

2. Enter your assigned UserID, i.e. a123456.
   - System response: *"PASSCODE:"*

   Note: *If system responds with "PASSWORD", the User ID you entered is not valid. Check to see if Caps Lock is activated.*

3. Enter the Startup PIN *(provided in the Login Information letter)* and current number displayed on the SecurID card in the format ppppnnnnnnn *(where p=pin and n=card display)*. Do NOT separate the two strings with a space or anything else.
   - System response: *"YOUR OLD PIN HAS EXPIRED, PLEASE CHOOSE A NEW ONE."*
     "OLD PIN:"

4. Enter the Startup PIN, i.e. **x604** *Do NOT include the numbers displayed on the SecurID card.*
   - System response: *"New PIN:"*

5. Enter new PIN, i.e. **2bme** *Do NOT include the numbers displayed on the SecurID card.*
   - System response: *"Re-enter New PIN:"*

6. Enter the new PIN again, i.e. **2bme** *Do NOT include the numbers displayed on the SecurID card*
   - System response: *"Last Login: ....."*
     "DESTINATION:"

7. Enter a destination name provided on your Login Information letter, i.e. **miaio**.
   - System response: *"Login prompt of destination."*

Logging In After the First Time

1. Dial-in to one of the ***Michigan Security Server*** modem pools. *(See Attachment B)*
   - System response: *"UserID:"*

2. Enter your assigned UserID, i.e. a123456.
   - System response: *"PASSCODE:"*

   Note: *If system responds with "PASSWORD", the User ID you entered is not valid. Check to see if Caps Lock is activated.*

3. Enter your PIN and current number displayed on the SecurID card in the format ppppnnnnnnn *(where p=pin and n=card display)*. Do NOT separate the two strings with a space or anything else.
   - System response: *"Last Login: ....."*
     "DESTINATION:"

4. Enter a destination name, i.e. **miaio**.
   - System response: *"Login prompt of destination."*

Shortcut Login Instructions

1. Dial-in to one of the ***Michigan Security Server*** modem pools. *(See Attachment B)*
   - System response: *"UserID:"*
2. Enter your assigned UserID a space and the desired destination name, i.e. a123456 miaio.
   - System response: *"PASSCODE:"*
3. Enter your PIN and current number displayed on the SecurID card in the format ppppnnnnnnn *(where p=pin and n=card display)*. Do NOT separate the two strings with a space or anything else.
   - System response: *"Last Login: ....."*
     "Login prompt of destination."

PIN Expiration Instructions

1. Dial-in to one of the ***Michigan Security Server*** modem pools. *(See Attachment B)*
   - System response: *"UserID:"*
2. Enter your assigned UserID, i.e. a123456.
   - System response: *"PASSCODE:"*

   Note: *If system responds with "PASSWORD", the User ID you entered is not valid. Check to see if Caps Lock is activated.*
3. Enter your PIN and current number displayed on the SecurID card in the format ppppnnnnnnn *(where p=pin and n=card display)*. Do NOT separate the two strings with a space or anything else.
   - System response: *"YOUR OLD PIN HAS EXPIRED, PLEASE CHOOSE A NEW ONE."*
     "Old PIN:"
4. Enter your PIN, i.e. **x604** *Do NOT include the numbers displayed on the SecurID card.*
   - System response: *"New PIN:"*
5. Enter new PIN, i.e. **2bme** *Do NOT include the numbers displayed on the SecurID card.*
   - System response: *"Re-enter New PIN:"*
6. Enter the new PIN again, i.e. **2bme** *Do NOT include the numbers displayed on the SecurID card*
   - System response: *"Last Login: ....."*
     "DESTINATION:"
7. Enter a destination name provided on your Login Information letter, i.e. **miaio**.
   - System response: *"Login prompt of destination."*

PIN Reset Instructions

1. Dial-in to one of the ***Michigan Security Server*** modem pools. *(See Attachment B)*
   - System response: *"UserID:"*
2. Enter your assigned UserID, i.e. a123456.
   - System response: *"PASSCODE:"*

   Note: *If system responds with "PASSWORD", the User ID you entered is not valid. Check to see if Caps Lock is activated.*
3. Enter your PIN and current number displayed on the SecurID card in the format ppppnnnnnnn *(where p=pin and n=card display)*. Do NOT separate the two strings with a space or anything else.
   - System response: *"Last Login: ....."*
     "DESTINATION:"
4. Enter the word **pin**.
   - System response: *"Old PIN:"*
5. Enter your PIN, i.e. **x604** *Do NOT include the numbers displayed on the SecurID card.*
   - System response: *"New PIN:"*
6. Enter new PIN, i.e. **2bme** *Do NOT include the numbers displayed on the SecurID card.*
   - System response: *"Re-enter New PIN:"*
7. Enter the new PIN again, i.e. **2bme** *Do NOT include the numbers displayed on the SecurID card*
   - System response: *"Last Login: ....."*
     "DESTINATION:"
8. Enter a destination name provided on your Login Information letter, i.e. **miaio**.
   - System response: *"Login prompt of destination."*

Ameritech Guest Login Procedures

It is now more convenient to access your systems/applications when traveling to other Ameritech locations outside of Michigan. Rather than a long distance call to Michigan, it is possible to log into the local SecurID NAS security system and then connect to the Michigan SecurID system. See *Attachment B* for a list of NAS Server Modem Pool numbers.

The following procedures guide you through the login process.

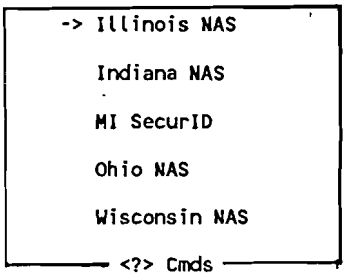
1. Dial-in to the local NAS modem pool *(See Attachment B)*
   - System response: *"Login:"*

2. Enter the Login **guest** and press the Enter key.
   - System response: *"Password:"*

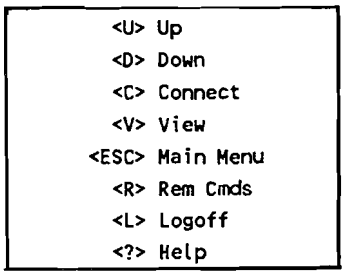
3. Enter **Ameritech1** and press the Enter key.
   - System response: *"Enter terminal type (default <vt100>) or <HELP>"*

4. Input your terminal type, or hit return if you want to select VT100, or type HELP to get a list of terminals.
   - If you select HELP, choose the appropriate terminal type and hit return.

5. A menu listing all Ameritech's SecurID security systems will appear, for example:



   - *To move forward in the menu, press the "F" key.*
   - *To move backwards in the menu, press the "B" key.*
   - *To get a full list of commands, press the Shift key and "?". The following menu will be displayed on the screen.*



6. Press the Enter key until the curser (-->) is next to MI SecurID, press the "C" key.
   - System response: *"Warning:.....*
     USERID:"

7. Follow *"Logging In After the First Time"* procedures.

Logging Off The NAS

1. If the user is at the NAS menu, press the "L" key, answer "Y" to disconnect the session.
2. If the user is in an application, enter the information required by the application to logoff the application. Note that the user will still need to logoff the network *(see step #1 above).*

Error Messages and Most Common Problems -Michigan Server

Message	Possible Cause
"password" prompt instead of "passcode"	- Make sure caps lock button is disabled for lower case input only. - Make sure your User ID was entered properly.
"login incorrect"	- Make sure caps lock button is disabled for lower case input only. - Make sure your User ID was entered properly. - Make sure passcode is entered with both the PIN and digits on the front of the SecurID card, no space. - If message persists, contact the Michigan SecurID Hotline.
"destination is unavailable"	- Dial-in ports to destination are all in use. Try again in a few minutes or try an alternate destination (i.e. Packet x.....), if available. - Network connections to destination or destination, may be down. Contact the Michigan SecurID Hotline. - User may be suspended for unsuccessful login attempts. Contact the Michigan SecurID Hotline for restoral.
"destination is not a valid destination"	- Make sure correct destination name is inputted. Verify destination name and try again. Valid destinations in user profile are found in the Login Information letter or contact the Michigan SecurID Hotline. - Destination not in user profile, contact appropriate Application Coordinator for destination desired and/or contact the Michigan SecurID Hotline.
"mrac1 or mrac2 not answering"	- Contact the Michigan SecurID Hotline.
No dial Tone	- Be sure that telephone wire from wall jack is plugged into modem jack in back of computer/terminal or modem. - Be sure that communication program is set to correct COMM PORT for modem, usually COMM 1.
Hung up in application	Openet application/system 1. Press Ctrl key] and press return. 2. At telnet> prompt type close and press return. 3. At telnet> prompt type quit and press return.
telnet>	Type **quit** and press the return key to return to the SecurID UserID prompt. DO NOT disconnect at this prompt.
"All Channels Busy"	Try accessing destination later. If message persists contact the Michigan SecurID Hotline.
"Remote Node Not Answering"	Contact the Michigan SecurID Hotline immediately.
"trunk in use" or "trunk is busy"	Contact the Michigan SecurID Hotline immediately.
"...LCS50E encountered an internal error.."	Contact the Michigan SecurID Hotline immediately.
Problems accessing **misna** destination	-Make sure the PC communication program you're using is SIMPC *(IBM compatibles)* or SIMMAC *(Macitosh)*. -At VTAM screen, did you type SIM5 to access MBT5? -Are you trying to access MBT5? If not, you must request access to the SNA Mainframe. This destination is only for MBT5 Users. Send an e-mail request to the Michigan SecurID Administration Center requesting SNA access.

SecurID Card Initialization -SNA

SecurID card initialization on the SNA Network can only be done if you've requested access to the SNA Network.

As soon as the user receives the SecurID card, they should notice whether or not the number displayed on the face of the card changes every 60 seconds. If not, the card is defective or damaged and should be returned to the SecurID Administrator.

Modem pools have been established in each state. Login instructions will depend on which telephone number is accessed. The users are responsible for understanding the nuances of their terminal or communication package setup. In some cases, the local CHC may be contacted for assistance.

USERID

The SecurID Administrator will establish a UserID for each user based on the Ameritech User Identification Standard, 16-350.

CARDCODE

The cardcode is the digits currently displayed on the front of the SecurID card.

Login Attempts

The user will have nine invalid attempts at the UserID/Cardcode screen before their card is disabled. If your card is disabled, contact the appropriate SecurID Administration Center Hotline to have the card re-enabled.

Ohio Access Instructions -*Cx80 Protocol Converter*

Modem PC/Terminal Setup	Terminal Type:	VT100	Data Bits:	7
	Baud Rate:	2400 Baud or less	Parity:	Even
			Stop Bits:	1

Keyboard Map *Attachment E.*

Access Number: **216-822-2931**

1. When connected, press the Shift key and } key until the following message appears.
   - System Response: *"** Cx-80 VER 04.83 **"*
     "USERID:"
     "CARDCODE:"
2. Input your UserID and press Tab key.
3. Input the numbers currently displayed on your SecurID card and press the Enter key.
   - System Response:

TERM: L1F0781F *TIME: 12:48 94.094*

****

AMERITECH ID: SECURID *MENU = 100*

WARNING!
THIS SYSTEM IS RESTRICTED TO AUTHORIZED PERSONS FOR AUTHORIZED BUSINESS PURPOSES. USERS MAY BE MONITORED TO PROPERLY ADMINISTER THE SYSTEM, TO IDENTIFY UNAUTHORIZED USE, AND TO INVESTIGATE MISUSE. CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED WITHOUT AUTHORIZATION.

TO USE => ENTER REGIONAL APPLICATION ID (APPLID) ONLY

ENTER X => RETURN TO SECURID AUTHENTICATION SCREEN

****

ENTER SELECTION ===>

4. Input the *Regional APPLID* of the system you wish to access and press the Enter key. For example, AAT3's Regional APPLID is ATTSO3.
   - System Response: *"CARDCODE APPROVED. PLEASE WAIT A MOMENT."*
     The Login Screen for the requested application/system.

Note: *Attachment C is a list of Regional Systems Information. The column labeled **TSO** is the Regional APPLID, the column labeled **SMFID** is the local APPLID. If the application or system you wish to access does not appear on this list, contact the appropriate application/system administrator for this information.*

Ohio Access Instructions -*Renex Protocol Converter*

Modem PC/Terminal Setup	Terminal Type:	VT100	Data Bits:	8
	Baud Rate:	9600 Baud or less	Parity:	None
			Stop Bits:	1

Keyboard Map *Attachment D.*

Access Numbers:	**216-384-3981**	**216-822-3062**	**216-822-5476**	**216-822-5477**

1. Once connected press the Enter key once.
   - System Response: *"Renex TMS-three, SN-00300974"*
     "Enter service code -"
2. Enter 1LU and press the Enter key.
   - System Response: *"Enter terminal type or "M" for menu -"*
3. Enter VT100 and press the Enter key.
   - System Response: *"USERID:"*
     "CARDCODE:"
4. Input your UserID and press Tab key.
5. Input the numbers currently displayed on your SecurID card and press the Enter key.
   - System Response:

TERM: L1F0781F *TIME: 12:48 94.094*
****
AMERITECH ID: SECURID *MENU = 100*

WARNING!
THIS SYSTEM IS RESTRICTED TO AUTHORIZED PERSONS FOR AUTHORIZED BUSINESS PURPOSES. USERS MAY BE MONITORED TO PROPERLY ADMINISTER THE SYSTEM, TO IDENTIFY UNAUTHORIZED USE, AND TO INVESTIGATE MISUSE. CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED WITHOUT AUTHORIZATION.

TO USE => ENTER REGIONAL APPLICATION ID (APPLID) ONLY

ENTER X => RETURN TO SECURID AUTHENTICATION SCREEN
****
ENTER SELECTION ===>

6. Input the *Regional APPLID* of the system you wish to access and press the Enter key. For example, AAT3's Regional APPLID is ATTSO3.
   - System Response: *"CARDCODE APPROVED. PLEASE WAIT A MOMENT."*
     The Login Screen for the requested application/system.

Note: *Attachment C is a list of Regional Systems Information. The column labeled **TSO** is the Regional APPLID, the column labeled **SMFID** is the local APPLID. If the application or system you wish to access does not appear on this list, contact the appropriate application/system administrator for this information.*

Illinois and Wisconsin Access Instructions -*Renex Protocol Converter*

Modem PC/Terminal Setup	Terminal Type:	VT100	Data Bits:	8
	Baud Rate:	9600 Baud or less	Parity:	None
			Stop Bits:	1

Keyboard Map *Attachment D.*

Access Numbers: **312-474-0250** **312-474-1146** **414-523-0529**
800-924-9127 *(Wisconsin Statewide access -excluding Milwaukee)*
800-453-0581 *(Outside Wisconsin)*

1. When connected, press the Enter key once.
   - System Response: *"Renex TMS-three, SN-00300974"*
     "Enter terminal type or "M" for menu -"
2. Enter VT100 and press the Enter key.
   - System Response:

     AMERITECH ID: L1F07811
     WARNING! THIS SYSTEM IS RESTRICTED TO AUTHORIZED PERSONS FOR AUTHORIZED BUSINESS PURPOSES. USERS MAY BE MONITORED TO PROPERLY ADMINISTER THE SYSTEM, TO IDENTIFY UNAUTHORIZED USE, AND TO INVESTIGATE MISUSE. CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED WITHOUT AUTHORIZATION.

   Note: *Generally the system will present you with the above screen. If not, you will be presented with the USERID, CARDCODE screen, skip to step 4 to continue.*
3. If this screen appears, type any alpha character and press the Enter key.
   - System Response: *"COMMAND ACCEPTED BY VTAM"*
     "USERID:"
     "CARDCODE:"
4. Input your UserID and press Tab key.
5. Input the numbers currently displayed on your SecurID card and press the Enter key.
   - System Response:

     TERM: L1F0781F *TIME: 12:48 94.094*
     ****
     AMERITECH ID: SECURID *MENU = 100*

     WARNING!
     THIS SYSTEM IS RESTRICTED TO AUTHORIZED PERSONS FOR AUTHORIZED BUSINESS PURPOSES. USERS MAY BE MONITORED TO PROPERLY ADMINISTER THE SYSTEM, TO IDENTIFY UNAUTHORIZED USE, AND TO INVESTIGATE MISUSE. CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED WITHOUT AUTHORIZATION.

     TO USE => ENTER REGIONAL APPLICATION ID (APPLID) ONLY

     ENTER X => RETURN TO SECURID AUTHENTICATION SCREEN
     ****
     ENTER SELECTION ===>
6. Input the *Regional APPLID* of the system you wish to access and press the Enter key. For example, AAT3's Regional APPLID is ATTSO3.
   - System Response: *"CARDCODE APPROVED. PLEASE WAIT A MOMENT."*
     The Login Screen for the requested application/system.

   Note: *Attachment C is a list of Regional Systems Information. The column labeled **TSO** is the Regional APPLID, the column labeled **SMFID** is the local APPLID. If the application or system you wish to access does not appear on this list, contact the appropriate application/system administrator for this information.*

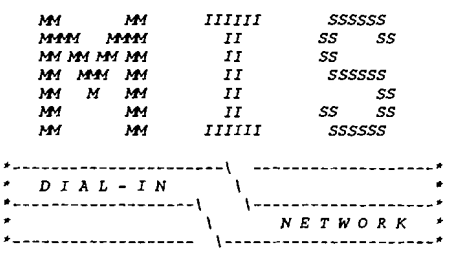
Michigan Access Instructions -*Cx80 Protocol Converter*

Modem PC/Terminal Setup	Terminal Type:	VT100	Data Bits:	7
	Baud Rate:	9600 Baud or less	Parity:	Even
			Stop Bits:	1

Keyboard Map *Attachment E.*

Access Number: **810-424-1868**

1. When connected, press the Shift key and } key until the following message appears.
   - System Response: *"** Cx-80 VER 05.04 **"*
     " Michigan Bell Telephone Company
     >>> COMMTEX Cx-80/PC-2 <<<



Press <ENTER> to continue..."

2. Press the Enter key.
   - System Response:

   AMERITECH ID: L1F07811
   WARNING! THIS SYSTEM IS RESTRICTED TO AUTHORIZED PERSONS FOR AUTHORIZED BUSINESS PURPOSES. USERS MAY BE MONITORED TO PROPERLY ADMINISTER THE SYSTEM, TO IDENTIFY UNAUTHORIZED USE, AND TO INVESTIGATE MISUSE. CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED WITHOUT AUTHORIZATION.

   Note: *Generally the system will present you with the above screen. If not, you will be presented with the USERID, CARDCODE screen, skip to step 4 to continue.*

3. If this screen appears, type any alpha character and press the Enter key.
   - System Response: *"USERID:"*
     "CARDCODE:"

4. Input your UserID and press Tab key.

5. Input the numbers currently displayed on your SecurID card and press the Enter key.
   - System Response:

   TERM: L1F0781F *TIME: 12:48 94.094*
   ****
   AMERITECH ID: SECURID *MENU = 100*

   WARNING!
   THIS SYSTEM IS RESTRICTED TO AUTHORIZED PERSONS FOR AUTHORIZED BUSINESS PURPOSES. USERS MAY BE MONITORED TO PROPERLY ADMINISTER THE SYSTEM, TO IDENTIFY UNAUTHORIZED USE, AND TO INVESTIGATE MISUSE. CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED WITHOUT AUTHORIZATION.

   TO USE => ENTER REGIONAL APPLICATION ID (APPLID) ONLY

   ENTER X => RETURN TO SECURID AUTHENTICATION SCREEN
   ****
   ENTER SELECTION ===>

6. Input the *Regional APPLID* of the system you wish to access and press the Enter key. For example, AAT3's Regional APPLID is ATTSO3.
   - System Response: *"CARDCODE APPROVED. PLEASE WAIT A MOMENT."*
     The Login Screen for the requested application/system.

Note: *Attachment C is a list of Regional Systems Information. The column labeled **TSO** is the Regional APPLID, the column labeled **SMFID** is the local APPLID. If the application or system you wish to access does not appear on this list, contact the appropriate application/system administrator for this information.*

Logging Off SNA

1. Log off your application/system. ***Illinois & Wisconsin access disconnects the session.***
   - System Responses ***(Ohio & Michigan)***: *"USERID:"*
     "CARDCODE:"
2. Disconnect your connection.

Error Messages and Most Common Problems -SNA

Message	Possible Cause
VTAM Access Delayed	Contact the local CHC.
No ports available still trying	Contact the local CHC.
Access rejected or Application not active	Contact the local CHC.
Can't get pass the USERID, CARDCODE screen	Did you enter your USERID correctly? Did you press the TAB key after entering your USERID? Did you request SNA access? If not, contact the appropriate SecurID Administration Center to verify access. Did you enter 9 or more invalid CARDCODE numbers? If so, your card may be disabled, contact the appropriate SecurID Administration Center. If none of the above, contact the appropriate SecurID Administration Center for assistance.
YOUR TIME TO RESPOND HAS EXPIRED....	You've reached the system inactivity threshold. Press the Enter key and enter your USERID and CARDCODE.
Connect to SecurID Modem & Protocol Converter & do not get USERID, CARDCODE screen	Contact the local CHC.

ATTACHMENT A

Ameritech

SecurID Card Request Form

(Print or Type)

AM860
(3-94)

New ☐ Temporary ☐ | Delete ☐ Update Application ☐ | Reissue ☐ | Reason: (Choose One) ☐ Expired ☐ Lost or Stolen ☐ Defective ☐ Damaged

REQUESTOR PROFILE

Name			Management ☐	Non-Management ☐	Contractor ☐	External Customer ☐	Vendor ☐
Title					Social Security		
Company Name	Address					Room	
City	State	Zip Code		Ameritech Standard UserID (If Known)			
Phone ( )	R.C. Code						
Requestors Signature						Date	
To be filled in by existing SecurID card holders:			SecurID Card Serial Number				
To be filled in by Temporary Users:			Return Card Date				

REQUEST APPROVAL (see coversheet, item #7 for explanation)

Name	Title		Social Security
Company name	Address	Room	
City	State	Zip Code	
Phone ( )	R.C. Code		
Approved Signature			Date

APPLICATION REQUEST

Application = Name of application, computer system, co switch, network address
Location = Illinois, Indiana, Michigan, Ohio, Region, Wisconsin

Application	Location (if known)	Application Coordinator Signature (when applicable)

FOR SECURID ADMINISTRATION ONLY

Date Received	Date Processed	Serial Number
User ID	First Mail Out Date	Second Mail Out Date

SecurID Card Request Form Instruction

AM 860
(3-94)

GENERAL INFORMATION

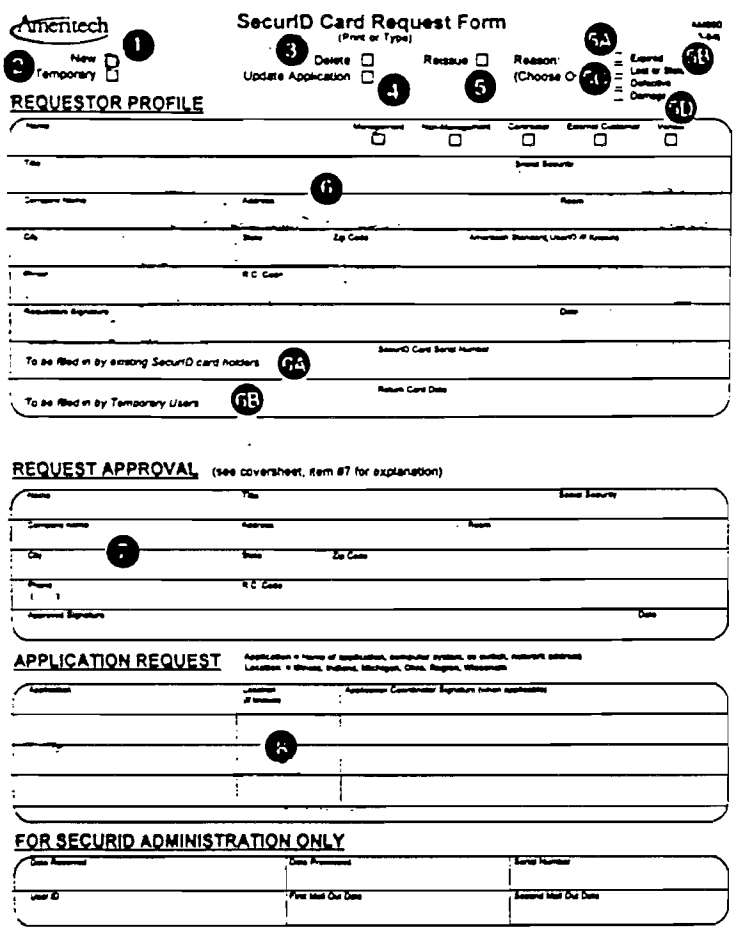
The SecurID card requestor must fill out the form completely, obtain appropriate approval signatures (Request Approval and Application Coordinator), retain user copy, and then forward form to the appropriate SecurID Administration group.
All non-Ameritech requestors require an Ameritech sponsor to obtain a SecurID card.
No form will be processed without ALL required signatures.
Please contact the appropriate SecurID Administration group with any questions. Mailing addresses and contact telephone numbers are listed below.

Illinois and Wisconsin

Ameritech- Distributed Security
Attn: SecurID Administration
225 W. Randolph, Room HQ9A
Chicago, IL 60606
Hotline: 312-727-8923
FAX: 312-727-4259

Indiana, Michigan, and Ohio

Ameritech- Distributed Security
Attn: SecurID Administration
23500 Northwestern Hwy., Room A220
Southfield, MI 48075
Hotline: 810-424-7505
FAX: 810-424-2550



1. **NEW** Check if this is a first time request for a SecurID card. "Request Approval" is required to obtain a new card.

2. **TEMPORARY** Check if SecurID card is required for less than 18 months. Requestor must indicate return date of card in "Requestor Profile". Request Approval" is required to obtain temporary card.

3. **DELETE** Check if SecurID card must be disabled and user deleted from SecurID security system due to retirement, dismissal, job transfer, leave of absence, etc. Return card with form. No "Request Approval" is necessary.

4. **UPDATE APPLICATION INFORMATION** Check if adding or deleting application(s) from user profile. "Application Coordinator(s)" approval may be required.

5. **REISSUE** Check if SecurID card needs to be reissued and then check the reason.

5A. **EXPIRED** Check if SecurID card is scheduled for expiration or has expired. IF the card has already expired, return with request form. No "Request Approval" is necessary.

5B. **LOST OR STOLEN** Check if SecurID card is lost or stolen. Report the card's loss *immediately* to the appropriate SecurID administration group. "Request Approval" is required to obtain another card.

5C. **DEFECTIVE** Check if SecurID card is defective. Return card with form. No "Request Approval" is required to obtain another card.

5D. **DAMAGED** Check if SecurID card has been damaged. Return card with form. "Request Approval" is required to obtain another card.

6. **REQUESTOR PROFILE** Complete ALL fields and include your payroll name and mailing address, sign, and date

6A. **Existing SecurID Card Holders** If you already have a SecurID card, you do not have to be issued another card. Provide the SecurID card's serial number.

6B. **Temporary Users** If you will be using your card for less than 18 months, provide return date.

7. **REQUEST APPROVAL** Ameritech employee's immediate supervisor must complete and sign this section to obtain a replacement for lost, stolen, damaged or defective cards. Non-Ameritech employees require an Ameritech sponsor's dated siganture for ALL card requests.

8. **APPLICATION REQUEST**
Application= Name of application, computer system, co switch, network address
State = Illinois, Indiana, Michigan, Ohio, Wisconsin (when applicable)
To obtain access to application(s) on the corporate networks, indicate the name of the application desired, location and the appropriate Application Coordinator's name and signature. Contact your local SecurID Administration group for Application Coordinator listing.

SecurID Modem Pool List

Modem Pools are 9600 auto baud, unless otherwise noted.

NAS Server

Illinois	312-368-0880	Chicago
	217-522-0091	Springfield
	708-259-2092	Arlington Heights
	708-653-0450	Wheaton
	815-722-2518	Joliet
Indiana	317-687-0333	Local/Long Distance
	1-556-4066	Indiana Official service
Ohio	216-384-2217	Akron
	216-223-6224	Cleveland
	614-223-4541	Columbus
	513-299-4648	Dayton *(1200 Baud)*
	419-245-7136	Toledo *(1200 Baud)*
	800-604-0700	*(Akron Intralata Only)*
	800-604-0800	*(Cleveland Intralata Only)*
	800-604-0900	*(Columbus Intralata Only)*
Wisconsin	414-344-1538	Milwaukee
	414-345-1537	Milwaukee
	800-254-0070	*(Milwaukee Intralata Only)*

SNA Mainframe

Illinois	312-474-0250	*Renex Protocol Converter*
	312-474-1146	*Renex Protocol Converter*
Michigan	810-424-1868	*Cx-80 Protocol Converter*
Ohio	216-384-3981	*Renex Protocol Converter*
	216-822-3062	*Renex Protocol Converter*
	216-822-5476	*Renex Protocol Converter*
	216-822-5477	*Renex Protocol Converter*
	216-822-2931	*Cx-80 Protocol Converter (2400 Baud)*
Wisconsin	414-523-0529	*Renex Protocol Converter*
	800-924-9127	Wisconsin Statewide access -excluding Milwaukee *Renex Protocol Converter*
	800-453-0581	Outside Wisconsin *Renex Protocol Converter*

Michigan Security Server

Detroit	313-496-8061	
Marquette	906-225-6602	
	800-521-6775	*(906 Intralata Only)*
Grand Rapids	616-776-9350	
	616-732-1943	*(2400 Baud)*
	800-924-3826	*(616 Intralata Only)*
	800-560-9998	*(616 Intralata Only -2400 Baud)*
Saginaw	517-776-4783	
	517-776-4194	*(2400 Baud)*
	800-246-1560	*(517 Intralata Only)*
	800-560-8181	*(517 Intralata Only -2400 Baud)*
Southfield	810-424-8620	
	810-424-0422	
	810-424-8822	*(2400 Baud)*
	810-424-8710	*(2400 Baud)*
	800-585-6241	*(313/810 Intralata Only)*
	800-585-6240	*(313/810 Intralata Only -2400 Baud)*

07/12/93 *(from B. Poltis)*

ATTACHMENT C

Regional System Information

Illinois

TSO	NV	SMIFID	SA	Shared DASD	NDM	NJE	Location
LATS01	LAN01	RM01	01		RM01	LANJE01	Riverfront-T
LATS02	LAN02	RM02	02	w/11, 1E	ILB02	LANJE02	Riverfront
A25TSO	LAN03	RM03	03		ASI1	A25JES	Riverfront
A04TSO	LAN04	MA04	04		ILB4	A04JES	Marquette Park
A06TSO	LAN06	SA06	06		ILB6	A06JES	Springfield
LATS07	LAN07	RM07	07		ILB24	LANJE07	Riverfront-T
A08TSO	LAN08	CC60	08	w/10,18,19,30	ILB08	A08JES	Canal
A10TSO	LAMFP	CD60	0A	w/8,18,19,30	ILB10	A10JES	Canal
A11TSO	LAN0B	RM11	0B	w/2,1E	ILB11	A11JES	Riverfront
A12TSO	LAN0C	TA12	0C	w/13,16	ILB12	A12JES	Canal
A13TSO	LAN0D	TB13	0D	w/12,16	ILB13	A13JES	Canal
LAVM0F		RV0F	0F	VM w/RV26	RV0F	A14RSCS	Riverfront
A18TSO	LAN12	DX18	12	w/8,10,19,30	DX18	A18JES	Canal
A19TSO	LAN13	DY19	13	w/8,10,18,30		A19JES	Canal
LATS14	LAN14	RM14	14				
A05VM		RV26	1A	VM w/RV0F	RV26	A05JES	Riverfront
LATS1B	LAN1B	RM27	1B		ILB1	LANJE27	Riverfront
LATS1C	LAN1C	RM1C	1C		ILB1C	LANJE28	Riverfront
LATS1D	LAN1D	RM1D	1D		ILB1D	LANJE29	Riverfront
LATS21	LAN21	RM21	21		ILB33	LANJE21	Riverfront
LATS4F	LAN4F	RM4F	4F		***	LANJE03	Riverfront
LATS50	LAN50	RM50	50	w/2,11,1E	*	RFT5	Riverfront-CMC

* ASI.Riverfront.1 ** ASI.Riverfront.2 *** ASI.Riverfront.3

Indiana

TSO	NV	SMIFID	SA	Shared DASD	NDM	NJE	Location
INTS01	NAN51	0181	51	Catlg 5	INB1	DPC1	Meridian
INTS04	NAN56	0480	56	Catlg 6	INB4	DPC3	Meridian
NATS53	NAN53	0581	53	Catlg 1	INB5	TIRKS1	Meridian
INTS06	NAN57	0683	57	Catlg 4	INB6	USER1	Meridian

Michigan

TSO	NV	SMIFID	SA	Shared DASD	NDM	NJE	Location
MITSO0	MAN96	MBT0	96	w/98p,9Dp	MBT0	BBLDG	Southfield
MITSO2	MAN98	MBT2	98	w/96P,9Ddp	MBT2	BBLDG	Southfield
MATS99	MAN99	SM99	99	w/9F,A3	*	SLD2	Southfield
MATS9A	MAN9A	SM9A	9A	w/A0p,A1p,A2p	***	SLD3	Southfield-CMC
VMCMS5	MIN05	MBT5	9B	VM w/9Cp	MBT5	MBT5	Southfield
MITSO6	MAN9C	MBT6	9C	w/9Bp	MBT6	TEST	Southfield
MITSO7	MAN9D	MBT7	9D	w/96P,98P	MBT7	BBLDG	Southfield
MATS9F	MAN9F	SM9F	9F	w/99,A3	*	SLD2	Southfield
ATTSO3	MANA0	AAT3	A0	w/9A,A1,A2	AAT3	AAT3	Southfield
ATTSO4	MABFP	SMA1	A1	w/9A,A0,A2	SMA1	SLD1	Southfield
MATSA2	MANA2	SMA2	A2	w/9A,A0,A1	**	SLD1	Southfield
MATSA3	MANA3	SMA3	A3	w/99,9F	*	SLD2	Southfield
MATSB2	MANB2	SMB2	B2		****	SLD4	Southfield

* ASI.Southfield.1 ** ASI.Southfield.2 *** ASI.Southfield.3 *** ASI.Southfield.4 p - means that the LPAR only shares some of the DASD on the other LPAR

Ohio

TSO	NV	SMIFID	SA	Shared DASD	NDM	NJE	Location
OBTS2	OAN66	D2SY	66	w/4	OBT1	CDC2	Brecksville
OBTS3	OAN67	SYS3	67	X		SYSTEM3	Brecksville-T
OBTS4	OAN68	B4SY	68	w/2	OBT1	CDC	Brecksville
OBTS5	OAN69	SYS5	69		OBT2	SYSTEM5	Akron-CMC
OATS6A	OAN6A	AM6A	6A	w/6B,6C	AM6B	AKN2	Akron
OATS6B	OAN6B	AM6B	6B	w/6A,6C	AM6B	AKN1	Akron
OATS6C	OAN6C	AM6C	6C	w/6A,6B	AM6B	AKN1	Akron-T
OATS6E	OAN6E	AM6E	6E			AKN4	Akron

x - datasets can also be accessed from OBTS4

Wisconsin

TSO	NV	SMIFID	SA	Shared DASD	NDM	NJE	Location
WATSCA	WANCA	PMCA	CA	w/CD,D1	PMCA	PWK1	Pewaukee
WATSCD	WANCD	PMCD	CD	w/CA,D1	PMCA	PWK1	Pewaukee
WATSCC-A	WANCC	PMCC	CC	w/CB	WBI1	HOWELL	Pewaukee
WATSCB-B	WANCB	PMCB	CB	w/CC	WBI1	HOWELL	Pewaukee
WATSC9-C	WANC9	1190	C9	w/D0,CF,DA	WBI3	PEWAUKEE	Pewaukee
WATSD0-F	WAND0	2290	D0	w/C9,CF,DA	WBI3	PEWAUKEE	Pewaukee
WATSD1	WAND1	PMD1	D1	w/CD,CA	PMCA	PWK1	Pewaukee
WATSD2	WAND2	PMD2	D2				Pewaukee
WATSD3	WAND3	PMD3	D3		**		Pewaukee
WATSCF-G	WANCF	PMCF	CF	w/C9,D0,DA	WBI3	PEWAUKEE	Pewaukee-D
WATSDA-H	WANDA	PMDA	DA	w/C9,D0,CF	WBI3	PEWAUKEE	Pewaukee-T
WATSFF	WANFF	PMFF	FF		*	PWK2	Pewaukee-CMC

* ASI.Pewaukee.2 ** ASI.Pewaukee.3