RSA SECURID® ACCESS
Implementation Guide

Cilasoft
Reinforced Authentication Manager for IBM (RAMi)

Peter Waranowski, RSA Partner Engineering
Last Modified: May 18th, 2018

RSA READY

Solution Summary

The Cilasoft Reinforced Authentication Manager for IBM I (RAMi) provides a RADIUS client on the IBM i platform which can integrate with RSA Authentication Manager and Cloud Authentication Service.

RAMi provides administrators with reinforced authentication services for the IBM i server to better secure user authentications.

The authentications can be configured dynamically to execute the request for additional user authentication via the RSA platform from the IBM i initial logon display, or can be added as part of an extra security layer inserted into user menus or into the logon procedure for individual applications such as access to ERP or financial systems via the Cilasoft API interface to RAMi.

RAMi runs natively on the IBM i platform as a C service program (*SRVPGM) object, and does not require any intermediary web services or the PASE environments to run. This means RAMi can be fully secured like any other IBM i application.

RAMi provides a simple way to map your existing IBM i user profiles to their corresponding RSA server user IDs. Additional Import scripts are available to do mass imports of SIDs from other systems.

The presentation of a Reinforced Authentication screen that accepts an RSA identification token to authenticate a user is driven by a set of configurable rules where you will choose which users or groups of users, which application jobs or calling program names or subsystems on your IBM i server will present users a field or screen to enter their RSA passcode.

The administrator can configure the authentication request to use just RSA passcodes, or to additionally require the IBM i password in order to access the system, or any protected applications or self-services.

When the RAMi self-services are configured and users are enrolled, this permits a user to perform 5250 green screen self-service of IBM i user profile re-enablement, and a self-service password reset to which access can be secured with the RSA Token interface.

RSA SecurID Access Features Cilasoft RAMi V5.43	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	-
SSO	
SAML SSO	-
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	-

RSA READY

Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

Cilasoft RAMi integration with RSA Cloud Authentication Service

Authentication Methods	REST	IDR SAML	Cloud SAML	HFED	RADIUS
RSA SecurID	-	-	-	-	✓
LDAP Password	-	-	-	-	✓
Authenticate Approve	-	-	-	-	✓
Authenticate Tokencode	-	-	-	-	✓
Device Biometrics	-	-	-	-	✓
SMS Tokencode	-	-	-	-	✓
Voice Tokencode	-	-	-	-	✓
FIDO Token		-	-	-	

Cilasoft RAMi integration with RSA Authentication Manager

Authentication Methods	REST	RADIUS	UDP Agent	TCP Agent
RSA SecurID	-	✓	-	-
AM RBA		-	-	

✓ Supported
\- Not supported
n/t Not yet tested or documented, but may be possible

Configuration Summary

All of the supported use cases of RSA SecurID Access with Cilasoft RAMi require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Cilasoft RAMi can be integrated with RSA Cloud Authentication Service in the following way:

RADIUS Client

Cloud Authentication Service RADIUS Configuration
Cilasoft RAMi RADIUS Configuration

RSA Authentication Manager – Cilasoft RAMi can be integrated with RSA Authentication Manager in the following way:

RADIUS Client

Authentication Manager RADIUS Configuration
Cilasoft RAMi RADIUS Configuration

RSA SecurID Access Configuration

RSA Cloud Authentication Service Configuration

RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to **Authentication Clients** > **RADIUS** > **Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**. Click **Publish** to push your configuration change to the RADIUS server.

RSA Cloud Authentication RADIUS server listens on port UDP 1812.

RSA Authentication Manager Configuration

RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Cilasoft RAMi with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Cilasoft RAMi components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Prerequisites

- You need to install a new instance of the Cilasoft product following the **"Cilasoft Products – Installation Guide – EN.pdf"**.
- You must also have the PSTF module "common tools" key installed. This is free with any Cilasoft module purchase.
- The Cilasoft Administrator who configures the RAMi rules and user mappings to be registered in Cilasoft as an "ADM" (Administrator) role, and must have *SECADM rights on the IBM i server.
- Cilasoft administrators without *SECADM rights on their IBM i profile will be refused from the RAMi menu and commands.
- To use the RAMi administration menus, please configure your 5250-device session to use 132-character wide screens (rather than the 80 character-wide screen default).

User IDs

You will need to map the SID known to RSA into the RAMi configuration for the corresponding IBM i user IDs. This can be done one by one in the early implementation phase.

For moving to production and enrolling many users, there is a configurable script import tool. To automate the process, you will need to find a way to match your IBM i users to the RSA SID users to each other. Often the user "Description" field can be used for this mapping if on both systems it contains the real user first and last names.

Some manual intervention could be required to review and validate the resultant mappings before importing them into RAMi.

Note: The full RAMi User Guide explains in detail how to configure rules and map user profiles.

Cilasoft RAMi RADIUS Client Configuration

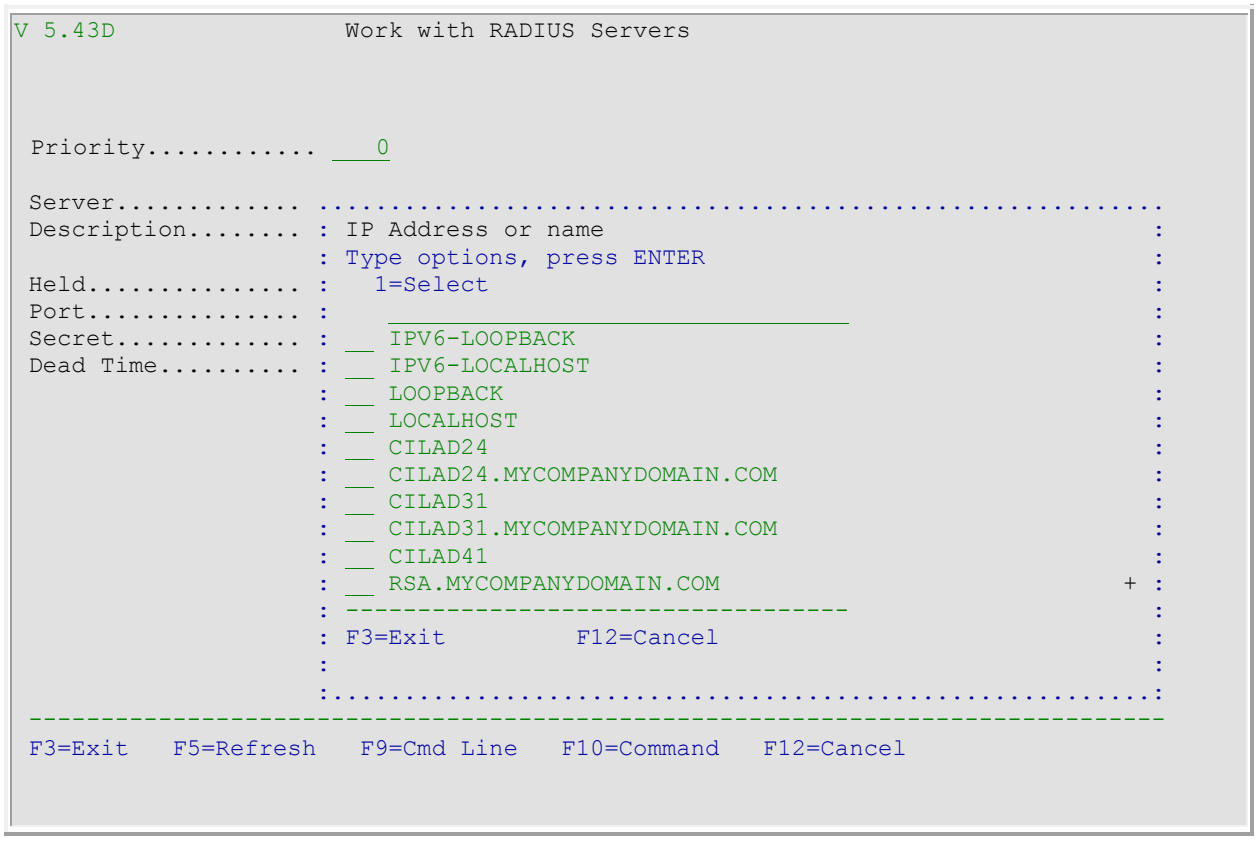
Complete the steps in this section to integrate with RSA SecurID Access using RADIUS authentication protocol.

Configure the IBM i to find the RSA Servers

1. Obtain the IP address(es) and full network name(s) of the RSA Server(s) on your network. The RSA Administrator can provide these details.
2. You will need the authority on the IBM i to run CFGTCP, and be enrolled as a Cilasoft ADM Administrator (WRKQJAUT to register yourself). Your user ID must also have *SECADM special authority to perform these tasks.
3. From CFGTCP menu use option 10 and ensure the RSA server is listed. If it is not there, use option 1 to add it. Test with the PING command to see if the IBM i server can reach the RSA Server.

```
                    Work with TCP/IP Host Table Entries
                                                          System:   CILAD22
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   7=Rename

     Internet                         Host
Opt  Address                          Name
 _   ___________________________________
 _   ::1                              IPV6-LOOPBACK
                                      IPV6-LOCALHOST
 _   127.0.0.1                        LOOPBACK
                                      LOCALHOST
 _   192.168.5.25                     RSA1.MYCOMPANYDOMAIN.COM
 _   192.168.5.91                     CILAD23
                                      CILAD23.MYCOMPANYDOMAIN.COM
 _   192.168.5.92                     CILAD24
                                      CILAD24.MYCOMPANYDOMAIN.COM
     192.168.5.93                     CILAD31
                                      CILAD31.MYCOMPANYDOMAIN.COM
 _   192.168.5.94                     CILAD21
                                                                  More...
F3=Exit   F5=Refresh   F6=Print list   F12=Cancel   F13=Sort by add sequence
F17=Position to        F22=Display entire field
```

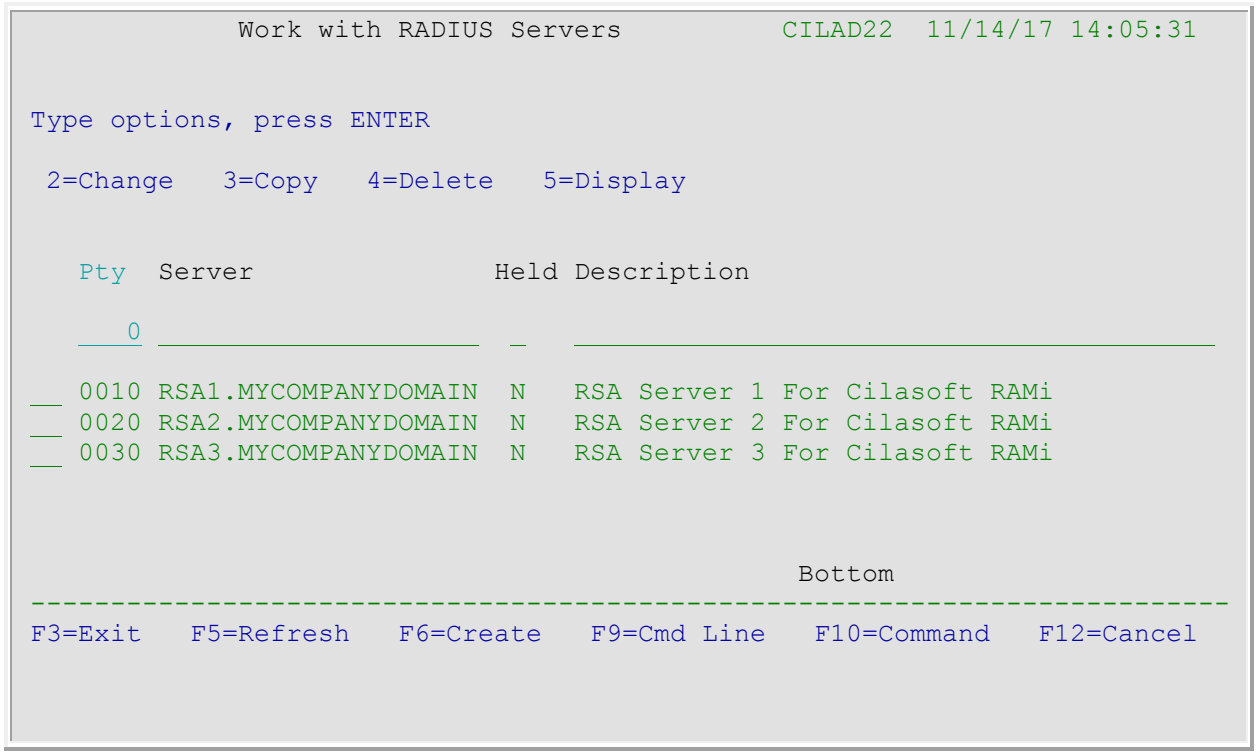
4. Use the Cilasoft command IJRN/WRKQASRV to define the RSA server in RAMi. Use F6 to create a new server.
5. Use F4 on the pink line; it will bring up a list of configured servers from your TCP/IP configuration Host Table Entries. Use the Filter on the top line, or page down to find or choose the RSA server.



6. In this example, the RSA server is called **rsa1.mycompanydomain.com** with IP of **192.168.5.25** and is set to priority 10

```
V 5.43D                  Work with RADIUS Servers

 Priority.............   10

 Server...............  RSA1.MYCOMPANYDOMAIN.COM

 Description.........  RSA Server 1 for Cilasoft RAMi

 Held.................  N (Y/N)

 Port.................  1645

 Secret..............  testing123

 Dead Time...........  2    seconds

 ------------------------------------------------------------------------------
 F3=Exit    F5=Refresh    F9=Cmd Line    F10=Command    F12=Cancel
```

- The server entry should be configured to use Radius port 1645 or 1812, whichever is the default UDP port on your network, as informed by the RSA or network administrator.
- Enter a description for the RSA Radius server, and enter the shared secret. This shared secret must match the value on the RSA Server configuration for the IBM i Cilasoft Client.
- This example shows "testing123" as the Secret – your shared secret should be different.
- The shared secret is encrypted in the RAMi server file and can only be viewed in clear text from this maintenance program.
- Deadtime is how long to ignore this server if it becomes non-responsive when re-checking the list of servers to process the login request. Default is 2 seconds - normally there is no reason to change this value.
- The priority is the order in which the servers will be interrogated to respond to the authentication request.



- You can enter multiple Radius servers in case of fail over, so there is always a server available to process a login. You can alternatively enter the IP address of a a load balancing server instead of using the RSA server directly.
- Cilasoft allows for up to 8 active RSA Servers in this release.

7. Using the command IJRN/WRKQJSET, review the default values for the following RAMi RADIUS parameters. In general, there is not a reason to change these values. If you are integrating with RSA Cloud Authentication RADIUS service you will need to update the LOGIN.TIMEOUT value. This is listed in seconds.
8. Use the Filter top line to show all the RADIUS related values.
9. The values for Group RAMI and member RADIUS are used to for extra parameters on the RADIUS servers.

```
SET10              Cilasoft settings                                  CILAD22
V 5.43.D                                                  11/14/17   14:05:15
Type options, press ENTER

 2=Change                        5=Display



   Group       Member      Keyword               Value

     %RADIUS%
   RAMI        RADIUS      DFT.REALM
   RAMI        RADIUS      LOGIN.TIMEOUT         60
   RAMI        RADIUS      SERVER.DEADTIME       120
   RAMI        RADIUS      SERVER.RETRIES        2
   RAMI        RADIUS      SERVER.TIMEOUT        5

------------------------------------------------------------------------
F3=Exit    F5=Refresh    F6=Create    F9=Cmd Line    F10=Command  F11=Next view
```

The RADIUS Dictionary in RAMi is called QADIC001. This file is stored in the IJRN library. If the records are missing or become corrupted, they exist in the QADICMDL model file, and can be copied using CPYF *REPLACE to correct the dictionary if required. RSA Communications will fail without the dictionary. This is a standard RADIUS dictionary file.

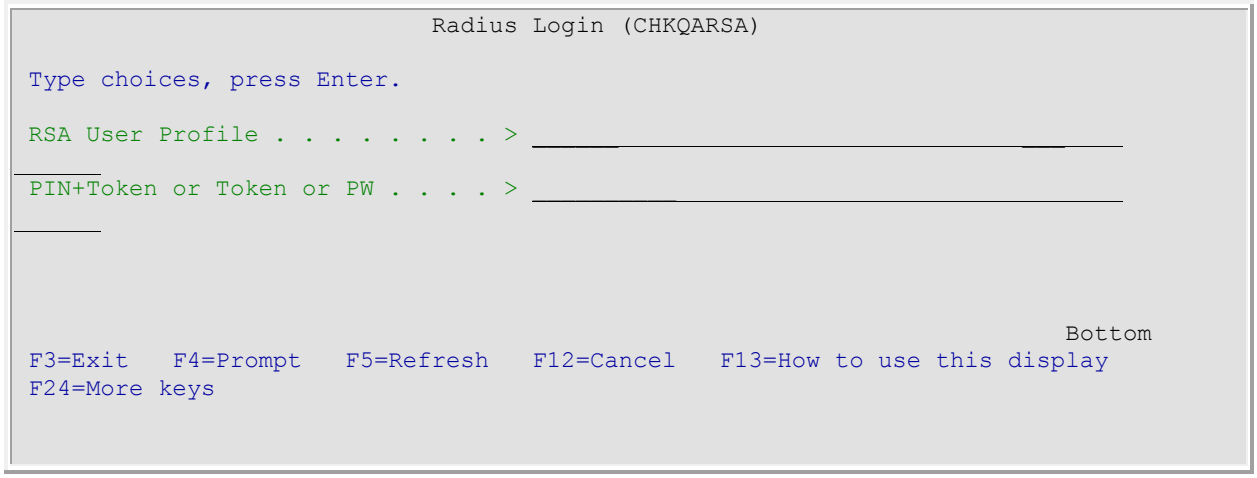
```
                                Display Physical File Member
File . . . . . :   QADIC001           Library  . . . . :   IJRNBC
Member . . . . . :   QADIC001         Record . . . . . :   1
Control  . . . . .                    Column . . . . . :   1
Find . . . . . .
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7..
#
# Updated 17/11/03 for release with Cilasoft RSA Radius Client.
#
#       This file contains dictionary translations for parsing
#       requests and generating responses.  All transactions are
#       composed of Attribute/Value Pairs.  The value of each attribute
#       is specified as one of 4 data types.  Valid data types are:
#
#       string - 0-253 octets
#       ipaddr - 4 octets in network byte order
#       integer - 32 bit value in big endian order (high byte first)
#       date - 32 bit value in big endian order - seconds since
#                                       00:00:00 GMT,  Jan.  1,  1970
#
#       Enumerated values are stored in the user file with dictionary
#       VALUE translations for easy administration.
#
#       Example:

F3=Exit    F12=Cancel    F19=Left    F20=Right    F24=More keys
```

Test IBM i Cilasoft Radius Client

The simple CHKQARSA tool has been provided so that you can first test that the basic server communications and token are working and obtain return codes before you proceed to configure the RAMi Rules and User profile mappings.

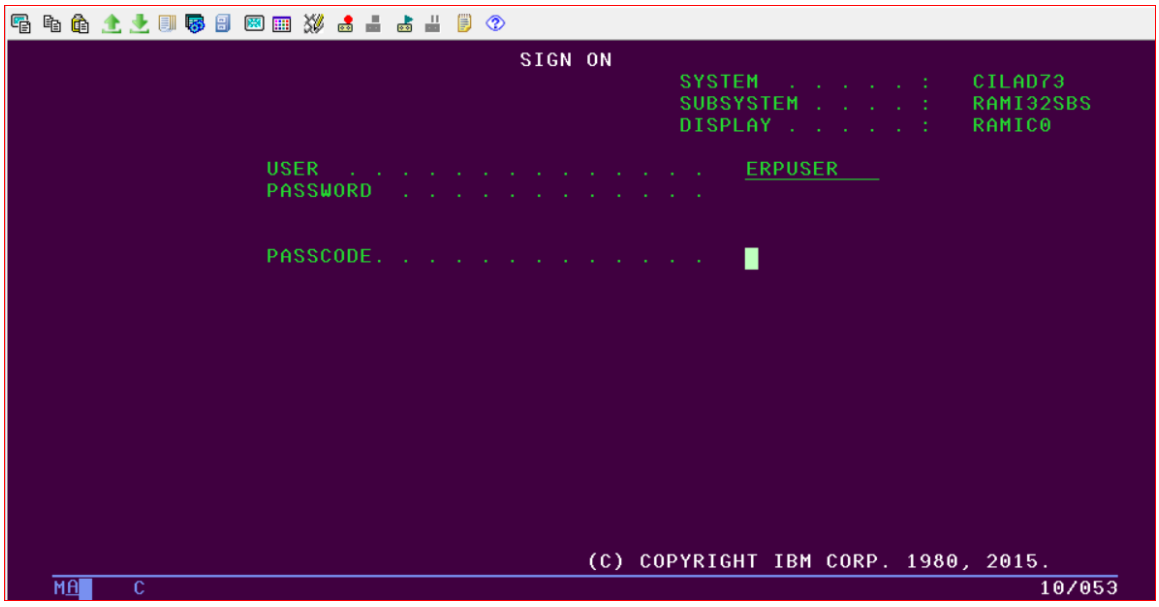
CHKQARSA

1. You must be a RAMi Administrator to use this tool – IJRN/CHKQARSA.
2. You must know an RSA user profile (as known in the RSA Security Console) and the corresponding pin + token code to test actual validation, PIN code changing etc.

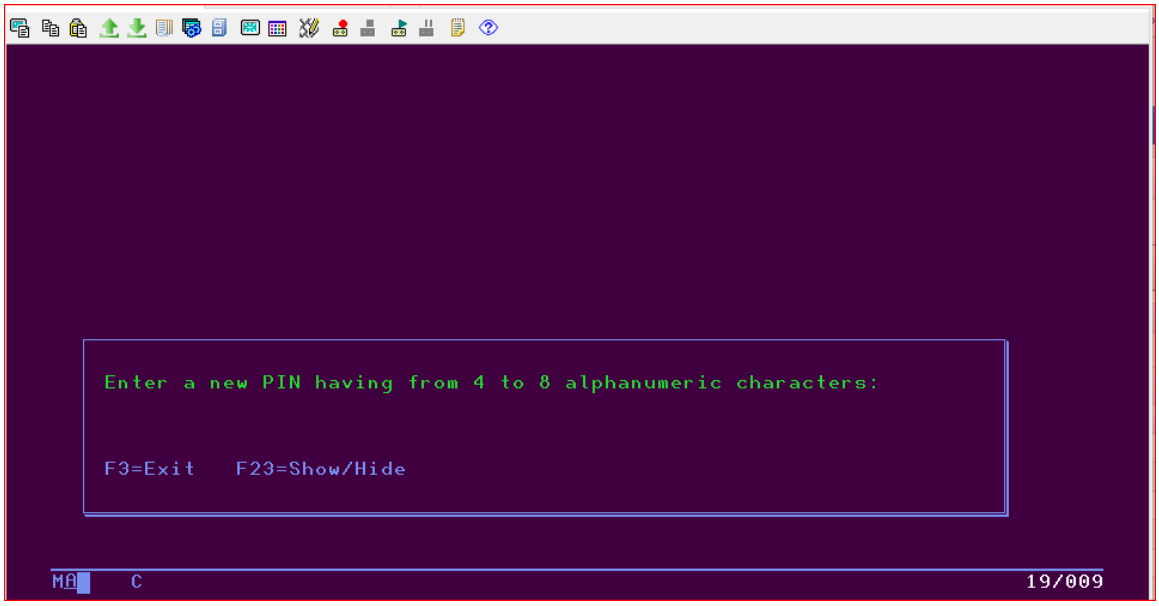


Login Screenshots

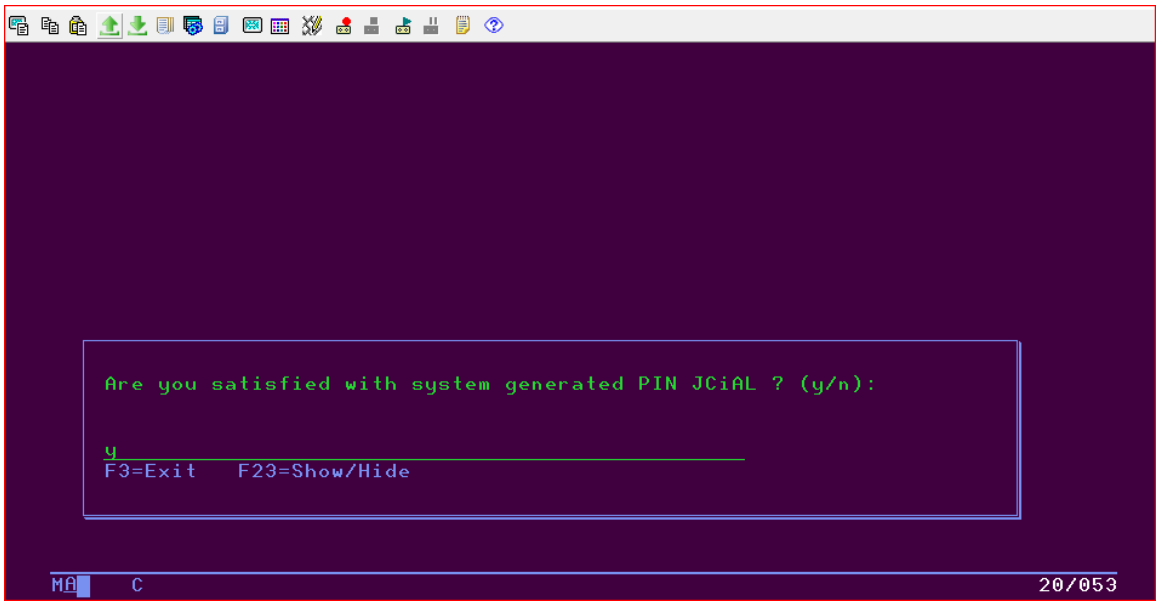
Login screen (AM):



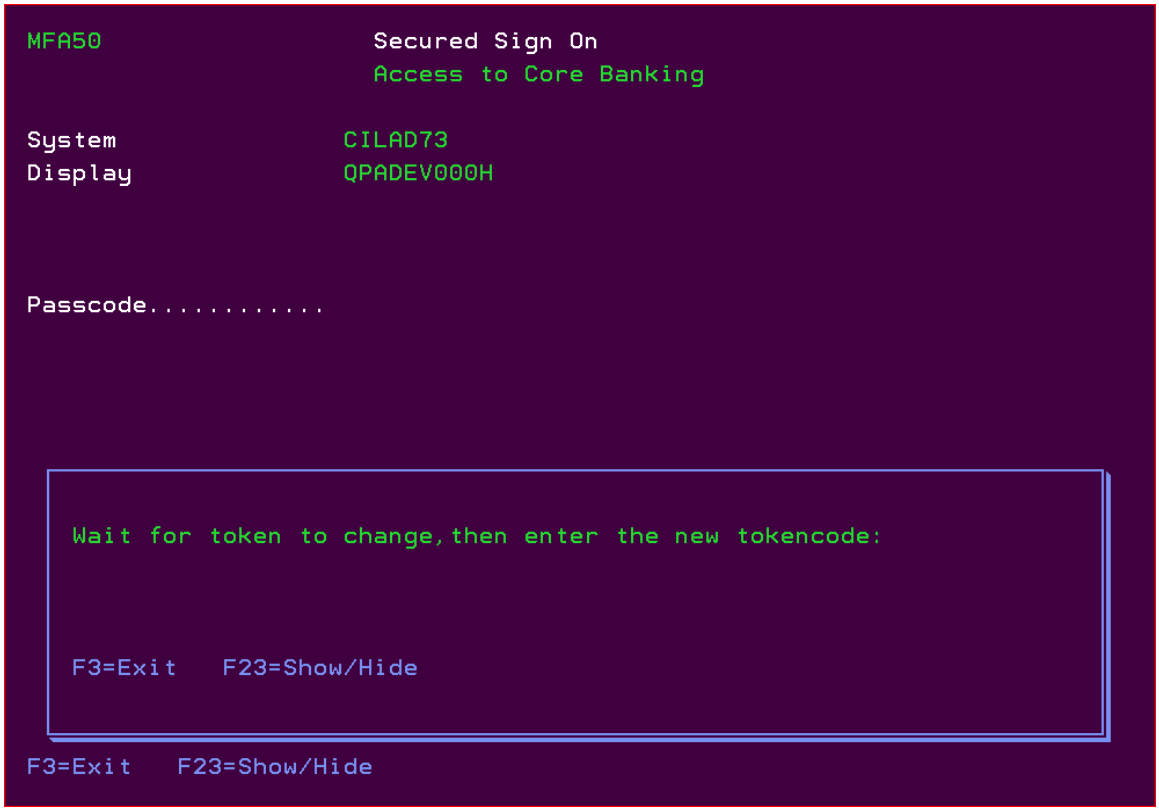
User-defined New PIN (AM):



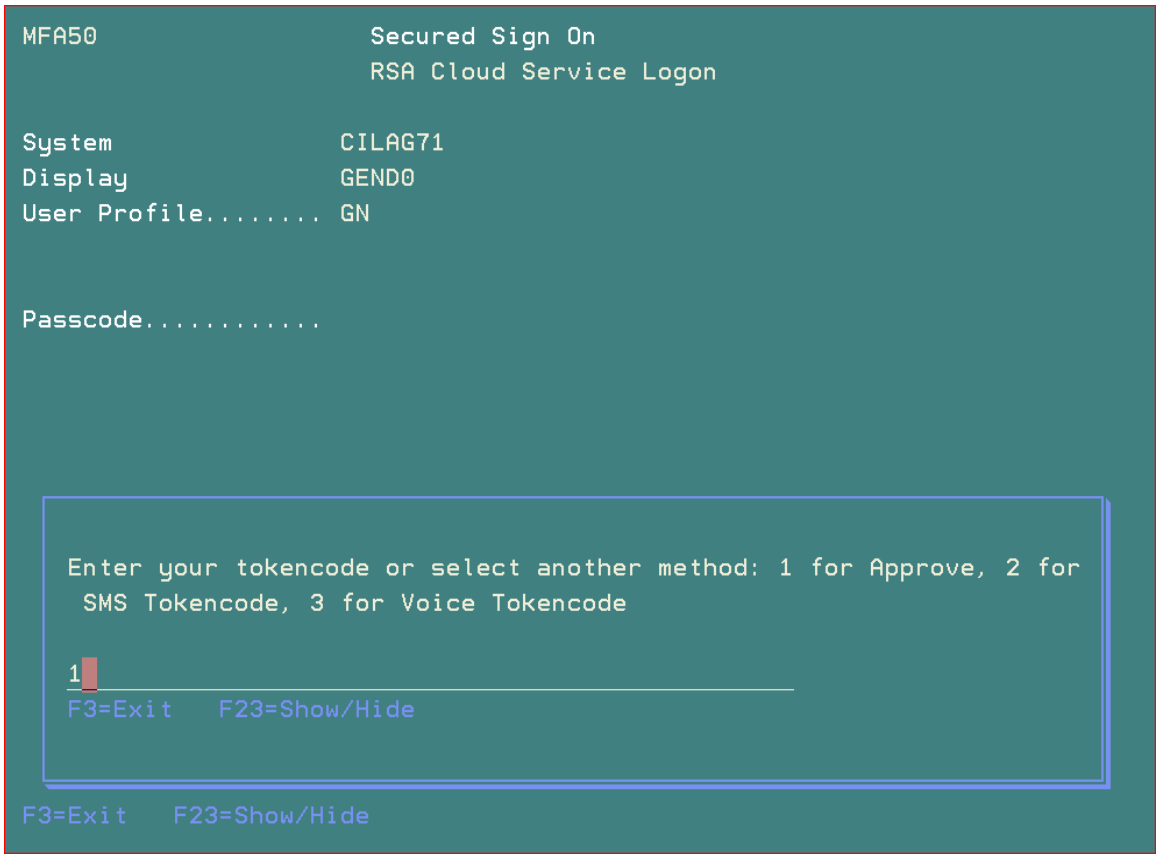
System-generated New PIN (AM):



Next Tokencode (AM):



Authentication Method Selection (Cloud):



Certification Checklist for RSA SecurID Access

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

Cilasoft RAMi V5.43.D

RSA Cloud Authentication Service

Date Tested: March 1st, 2018

Authentication Method	REST Client	RADIUS Client
RSA SecurID	-	✓
LDAP Password	-	✓
Authenticate Approve	-	✓
Authenticate Tokencode	-	✓
Device Biometrics	-	✓
SMS Tokencode	-	✓
Voice Tokencode	-	✓
FIDO Token	-	

RSA Authentication Manager

Date Tested: February 27th, 2018

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	-	-	-	✓
RSA SecurID Software Token Automation	-	-	-	-
On Demand Authentication	-	-	-	✓
Risk-Based Authentication		-		-

✓ = Passed, **X** = Failed, **-** = N/A

Appendix

RSA SecurID Access Integration Details

Partner Integration Details	
RSA Authentication Agent API (UDP)	N/A
RSA Authentication Agent API (TCP)	N/A
RSA SecurID Authentication API	N/A
RSA SecurID User Specification	Designated Users
Display RSA Server Info	Yes
Perform Test Authentication	Yes
Agent Tracing	N/A