

SECTION 13: ON-AIR AUTHENTICATION

In some situations, you may be required to authenticate with another station. For example, if you are transmitting mission-critical information or instructions and the receiving station needs to make sure you are actually an authorized ARES station, the receiving station will ask you to authenticate.

Once you complete this section, you will be able to:

- Request authentications from other stations
- Respond to requests for authentication
- Change to new code tables
- Resolve authentication failures.

The process of authentication is simple. The station that requests the authentication chooses a challenge code at random from a code table (a printed matrix of unique, secret codes called a one-time pad). The station that has been challenged to authenticate has the same code table, and finds the matching response code. The challenged station reads the response back to the challenger, who then checks their code table to ensure that the response is correct. If the response is correct, the challenger knows that the challenged station has the correct code table and is therefore authorized to send or receive traffic.

Most ARES stations will be provided with a standard set of code tables. For specific high-sensitivity links between specific stations (for example, between an EOC and a command centre), additional code tables may be provided that are available only to those stations, providing an extra layer of authentication. (For procedures regarding *restricted authentication*, see the Communications Station Operating Procedures at your post, if available.)

Table 2: Example code table for challenge-response station authentication

Authentication codes - sheet 3 - issued 2004-08-01					
Challenge	Response	Challenge	Response	Challenge	Response
388	11C8EJ	6MN	29IX9K	DJY	DIDJ3I
4JJ	CEWWN C	A3J	329I2D	F22	5KXKW N
58C	R2IMCK	A9N	OKPOKX	FT4	CUI4KS
5SI	NNREKS	BQL	JICWOE	H0J	C4ID99
683	TE3JC8	CLL	DJCFIJ	Q90	KLKZLK

Codes are sorted numerically and alphabetically, down the left column, then down the middle column, and then down the right column.

Any authentication code is used only once. All stations that hear an authentication (even if they are not participating) cross out the challenge-response code on their code table so that the code is not used again.

When most of the codes on a code table have been used, the net controller will retire the pad, asking all stations to begin using the next pad in the series.

The following procedures will help you perform authentications. Suggested on-air scripts are provided, but you can use your 'own words' so long as the overall protocols are followed.

Procedure 13-1: Request authentication from another station



Do not overuse authentication: Request authentication only when demanded by the traffic you are sending, at the request of the originator or recipient, or if you have reason to believe that you are being 'spoofed'. During an emergency, not all ARES stations will have current code tables, and some stations may have only a limited number of code tables. Once a code is used by any station, it cannot be reused. In addition, a repeated failure of a station during authentication usually results in the disposal of the current code table by all stations. Authentication should be an exceptional event that happens primarily during the set-up of operations, and not routinely.

1. If you have been off-net for a period of time (either off the air or on a frequency without a net controller), check in to the primary net or a secondary net and ask for confirmation of the current code table. The net controller will read out the current code table's sheet number and date (found in the upper left section of the table). Make sure that you are using the code table that the net controller identifies. Return to your working channel.

2. Pick an unused challenge-response pair from the current code table.

3. Ask the other station to authenticate, and read the challenge code. *For example, say, "VE9FK, this is VE9ZYX, please authenticate, Whiskey-8-3"*.
4. Stand by while the other station looks up the response on their code table.
5. If the other station responds, "Challenge expired," cross the challenge-response code off your code table and return to [Step 2](#).
6. If the other station responds, "Challenge not found," compare the sheet number and date they read you with the sheet number and date on your own code table. If your code table is 'newer' than theirs, ask them to update to the new code table. If your code table is 'older', update your own code table to match theirs. Then return to [Step 2](#).
7. If the other station reads back a response code, validate it using your code table.
8. Cross off the challenge-response pair on your code table so you do not use it again.
9. If the response is valid, reply "Authenticated", and proceed with traffic handling.
10. If the response is not valid and you have tried to authenticate less than three times, return to [Step 2](#) and try again.
11. If you have tried three times without success, reply "Authentication failed", and go to [Procedure 13-3: "Responding to an authentication failure"](#).

Procedure 13-2: Respond to a request for authentication from another station

1. When you are asked to authenticate, write down the challenge code and look it up on your code table.
2. If the challenge code is crossed out (meaning it has already been used), respond, "Challenge expired, please try again", and return to Step 1.
3. If you cannot find the challenge code on your code table, respond, "Challenge not found," then read back the sheet number and date of your code table (see the upper left section of the table), and return to Step 1.
4. Reply to the challenging station with the response code that appears beside the challenge code in the code table.
5. Stand by while the challenging station verifies your response.
6. If the challenging station asks you to authenticate again, return to Step 1.

Procedure 13-3: Responding to an authentication failure

1. If you are a net controller, go to [Procedure 13-7: "Resolving authentication failures"](#).
1. If you are not on a net controlled channel, ask the failed station to move to the primary net for follow-up, and then go to the primary net yourself.

-
2. Ask the net controller for assistance to resolve an authentication failure.

 3. If you are asked by the net controller for the issue number of your code table, read back the sheet number and date from the upper left portion of the table.

 4. If you are asked by the net controller to change to a new code table, securely destroy your current code table and open the new code table contained in your code table envelope.

 5. Follow any other instructions provided by the net controller.

Procedure 13-4: Monitoring a challenge-response between other stations

1. Each time a challenge code is used, find it on your code table and cross it out. This ensures that you do not use that code yourself later on.

2. If a challenge-response fails, make a note of the callsign of the failed station. (If you are required later to communicate with the station that failed authentication, you may want to authenticate them yourself.)

3. If your code table has only three unused codes remaining and you are on a frequency without a net controller, move temporarily to the primary net and notify the net controller that a new code table is required.

4. If you are a net controller on a secondary net and your code table has only three unused codes remaining, contact the net controller on the primary net (either directly on a second transceiver, or using a relay station) and notify them that a new code table is required.

5. If you are the net controller on the primary net and your code table has only three unused codes remaining, or you are notified by another station that a new code table is required, go to [Procedure 13-5: "Ordering a change to a new code table"](#).

Procedure 13-5: Ordering a change to a new code table

Use this procedure if you are the net controller on the primary net and your code table has only three unused codes remaining, or you are notified by another station that a new code table is required, or you decide to order a new code table to resolve an authentication failure (which might occur if two stations are using different code tables).

-
1. Securely destroy your current code table.

 2. Take the next code table sheet out of your code table envelope.

 3. Write down the sheet number and date of the new code table (see the upper left section of the code table).

 4. Broadcast an instruction to all stations on the primary net, asking them to change to the new code table with that specific sheet number and date.

-
5. If there are secondary nets in operation, contact the secondary net controllers directly using a second transceiver, or by way of a relay station, and ask them to make the same request to their net stations.
-

Procedure 13-6: Changing to a new code table

Use this procedure when you are asked either by a net control station or a challenging station to change to a new code table.

-
1. Write down the sheet number and issue date of the new code table.
 2. Securely destroy your current code table.
 3. Remove the new code table (identified by its sheet number and issue date) from your code table envelope.
 4. Begin using the new code table immediately for any authentications.
-

Procedure 13-7: Resolving authentication failures

Use this procedure if you are an active ARES net control station and are requested by another station to resolve a failure to authenticate.

-
1. Get both stations on frequency together.
 2. Query both stations for their code table sheet number and date.
 3. If one of the stations is using an incorrect code table, ask them to update to the current code table and try again.
 4. If you suspect an operator competence problem (for example, if an operator has been on duty for an extended period at the failed station and is exhausted), consider asking the failed station to change operators, to go off-air and take a break, or to cease operations.
 5. If you suspect that spoofing or malicious interference may be taking place, cease communications with the failed station and broadcast an alert regarding the situation to all stations involved in the ARES operation.
-