```
0699  # Note that although the authenticators aren't explicitly restricted
      # to the submission service, they are only used in that case because
0701  # only the submission service has a TLS certificate, and the MUA
      # server only sends messages via the submission service.
0703
      begin authenticators
0705
      # We could be vulnerable to password stealing by spammers, so it's
0707  # important that the authentication mechanisms are reasonably secure.
      # We protect passwords from snooping by requiring TLS, and the
0709  # password-changing program checks for basic password security.
      # TLS is only advertised if we have a certificate available, and we
0711  # only have certificates for the message submission service.

0713  LOGIN:
        driver                  = plaintext
0715    server_set_id           = $1
        server_prompts          = <| Username: | Password:
0717    server_condition        = \
              ${if crypteq{$2}{${lookup {$1} cdb {USERS/passwd.cdb} }} }
0719    server_advertise_condition = ${if !eq{}{$tls_cipher} }

0721  PLAIN:
        driver                  = plaintext
0723    server_set_id           = $2
        server_prompts          = :
0725    server_condition        = \
              ${if crypteq{$3}{${lookup {$2} cdb {USERS/passwd.cdb} }} }
0727    server_advertise_condition = ${if !eq{}{$tls_cipher} }

0729  # This authenticator is used to communicate authentication from the
      # central MUA server to us for bounce address tagging. EXTERNAL is a
0731  # standard SASL mechanism that uses external information to
      # authenticate the stated username; in this case the external
0733  # information is that we trust the client, i.e. the MUA server.
      # The mechanism is only advertised to the MUA server.
0735
      EXTERNAL:
0737    driver                  = plaintext
        server_set_id           = $1
0739    server_prompts          = :
        server_condition        = yes
0741    server_advertise_condition = ${extract {mua}{SENDER_PARAM} }
```