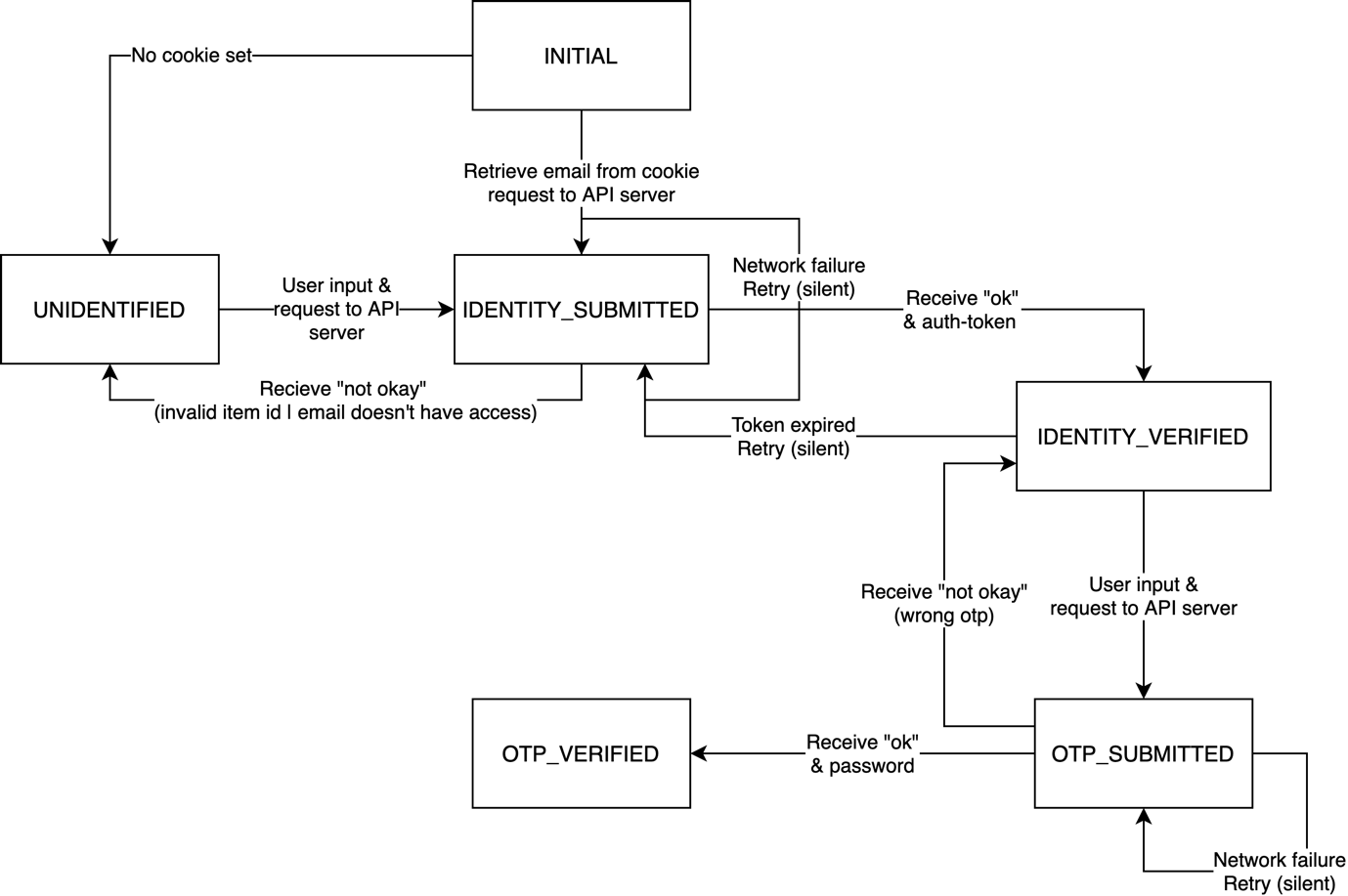
As only a GET request can be generated from within the email, put the uuid/item\_id in the query string. i.e. [https://se.secureage.com/?id=${uuid/item\_id}](https://se.secureage.com/?id=$%7buuid/item_id%7d).



# States

## INITIAL

In the initial state the frontend server should have already injected the uuid/item\_id in to the application state.

* IDENTITY\_SUBMITTED:
  + Cookie exists & email address is retrieved from it
  + Request is sent to API server
* UNIDENTIFIED
  + Otherwise

## UNIDENTIFIED

In the unidentified state the user should be prompted to enter the email address for which he received the encrypted email.

* IDENTITY\_SUBMITTED:
  + User has entered email address
  + Request is sent to API server

## IDENTITY\_SUBMITTED

In the identity\_submitted state, frontend waits for response from server

* IDENTIFY\_VERIFIED:
  + Receives a response with of “okay” status
  + Response has auth\_token in the body
* UNIDENTIFIED:
  + Receives a response with “not okay” status
* IDENTITY\_SUBMITTED:
  + Network failure, silent retry

## IDENTITY\_VERIFIED

In the identity\_verified state, user should be prompted to check his email for OTP.

* OTP\_SUBMITTED:
  + User has entered the OTP
  + Request is sent to API server
* IDENTITY\_SUBMITTED:
  + Token expired (expiry is given in previous response)
  + Silent retry?

## OTP\_SUBMITTED

In the otp\_submitted state, frontend waits for response from server.

* OTP\_VERIFIED:
  + Receives a response with “okay” status
  + Response has the password in the body
* IDENTITY\_VERIFIED:
  + Receive a response with “not okay”

## OTP\_VERIFIED

In this final state, simply display the password.