CAS Protocol v1.0
Authentication Example

1. User requests a resource on MyVT that requires authentication.

2. MyVT redirects to CAS server for authentication.
   https://auth.vt.edu/login?service=http://my.vt.edu,

3. /login URL displays a form for the user to enter authentication credentials. A hidden field called it contains the login ticket to thwart replay attacks.

4. The user submits the authentication credentials back to the /login URL via HTTP POST. This step MUST be encrypted.

5. Authentication success?
   5a. Yes, Redirect to http://my.vt.edu?ticket=ST-XXXXX...
The ticket parameter is a one-time-use service ticket that is sent in the clear and must be subsequently sent to CAS for validation. Optional setting of ticket-granting cookie to facilitate single sign-on.
   5b. No. Redirect to /login URL to display authentication failed message. Option to allow subsequent tries for authentication.

6. Service ticket valid?
   Yes
   6a. Destroy internal record of service ticket to fulfill single-use requirement.

7. CAS server returns text/plain response indicating service ticket validity.

6. MyVT sends service ticket delivered in step 5 to CAS for validation:
   https://auth.vt.edu/validate/?ticket=ST-XXXXX...

CAS Server @
https://auth.vt.edu