|  |
| --- |
| Use Case: Authenticate User |
| ID: 1 |
| Brief Description: The user presents his/her credentials to the Veni App, which are forwarded to the Veni System Server. Once verified, a user’s session can start. |
| Note: This is an “Included” –only use case. |
| Primary Actors: Veterans |
| Secondary Actors: None |
| Preconditions: A veteran has downloaded the Veni app and run through the “first run experience” (see Use Case: “First Run Experience” (1)) |
| Main Flow:  1. The Veni App will provide a standard UI to which the user will provide his credentials 2. The user will provide his credentials 3. The Veni App will transfer the credentials to the Veni Server 4. The server will validate the credentials, fetch the user’s information (including his/her identifying tokens to the VistA system), creating the user’s session 5. The server will send session initiation information to the Veni app. |
| Post Conditions: The veteran is authenticated, the Veni System Server has created a session for him that includes the information needed to communicate to the VistA system on his/her behalf |
| Alternative Flows:  1. If the veteran does not provide credentials within a reasonable time, the Veni App will transfer to a “Welcome” screen, requiring a new authentication effort from the user 2. The system does not include account lockout, but repeated authentication failures will result in longer wait times between authentication attempts – an “anti-hammer” rather than lock-out strategy |