Sequence diagram — Participants: User, User Agent, Client server-based, AA Server, User Directory

- User → User Agent: **Request client application**
- User Agent → Client server-based: Request Client Application website
- Client server-based ⇠ User Agent: return website
- User Agent ⇠ User: display website
- User → User Agent: **Click login button**

**opt** — Authentication JWT is present
- User Agent → AA Server: User access request(JWT, client ID, callback URL, scopes)
- AA Server: Verify JWT
- AA Server ⇠ User Agent: Return JWT validity

**alt** — Authentication JWT is not present OR Authentication JWT is invalid
- User Agent → AA Server: User access request (client ID, callback URL, scopes)
- AA Server: Validate client id
- AA Server ⇠ User Agent: Provide login form
- User Agent ⇠ User: Display Login form
- User → User Agent: Enter UID
- User Agent → AA Server: Send user details (UID)
- AA Server → User Directory: Request login challenge
- User Directory: Generate challenge
- User Directory ⇠ AA Server: Response (Challenge)
- AA Server ⇠ User Agent: authenticatorGetAssertion
- User Agent ⇠ User: Prompt user to use authenticator
- User → User Agent: Use authenticator
- User Agent → AA Server: AuthenticatorAssertionResponse
- AA Server → User Directory: Forward response + UID
- User Directory: Validate response against UID
- User Directory ⇠ AA Server: Return credential validity
- AA Server ⇠ User Agent: Return authentication JWT

Authentication JWT is valid
- *(No further steps in this stage)*

**Post-conditions:** The user has been authenticated with the AA Server. AA Server may proceed to evaluate access policy, issue tokens etc.