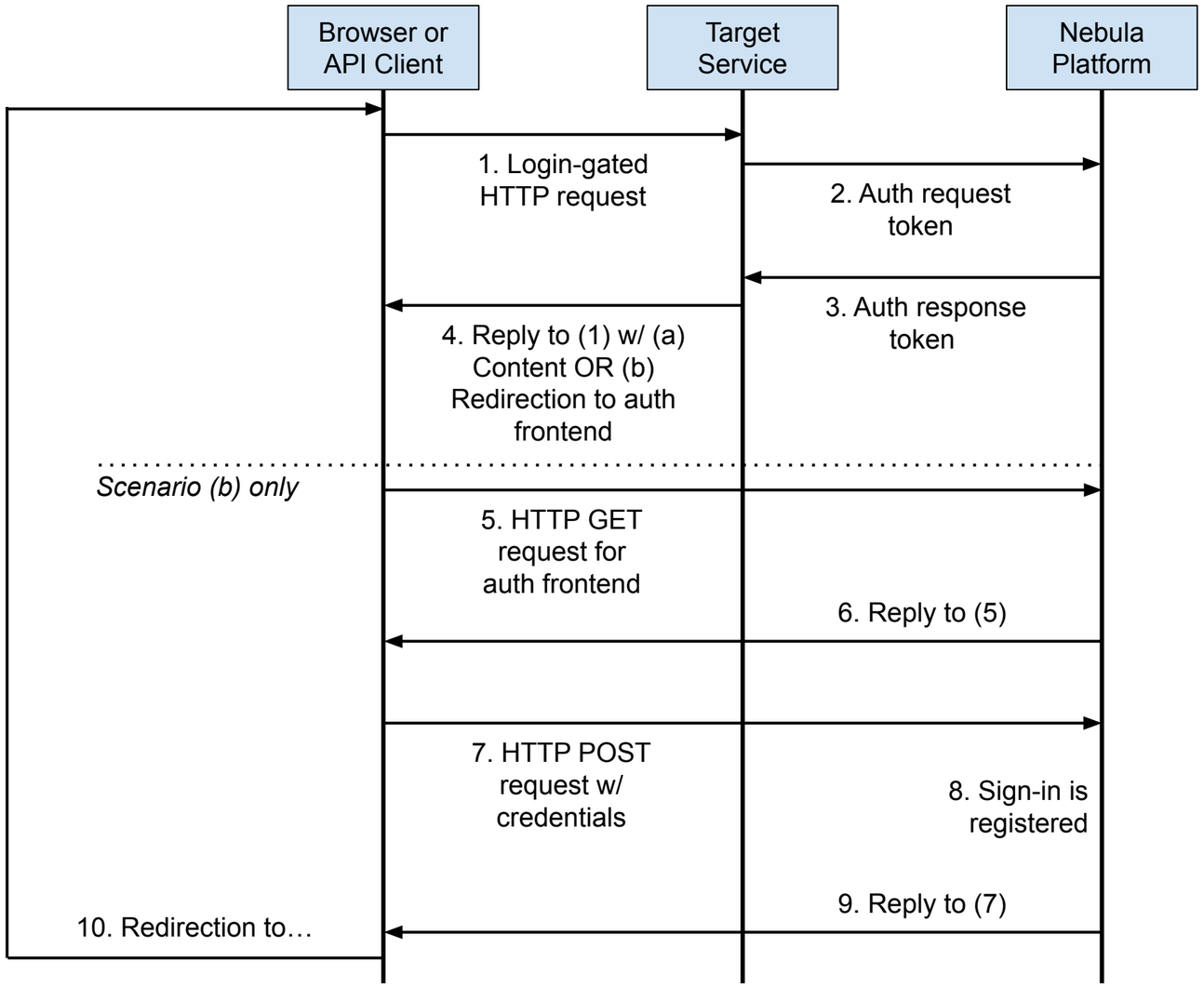
Centralized Approach (Authority comes from DB) (Bad)



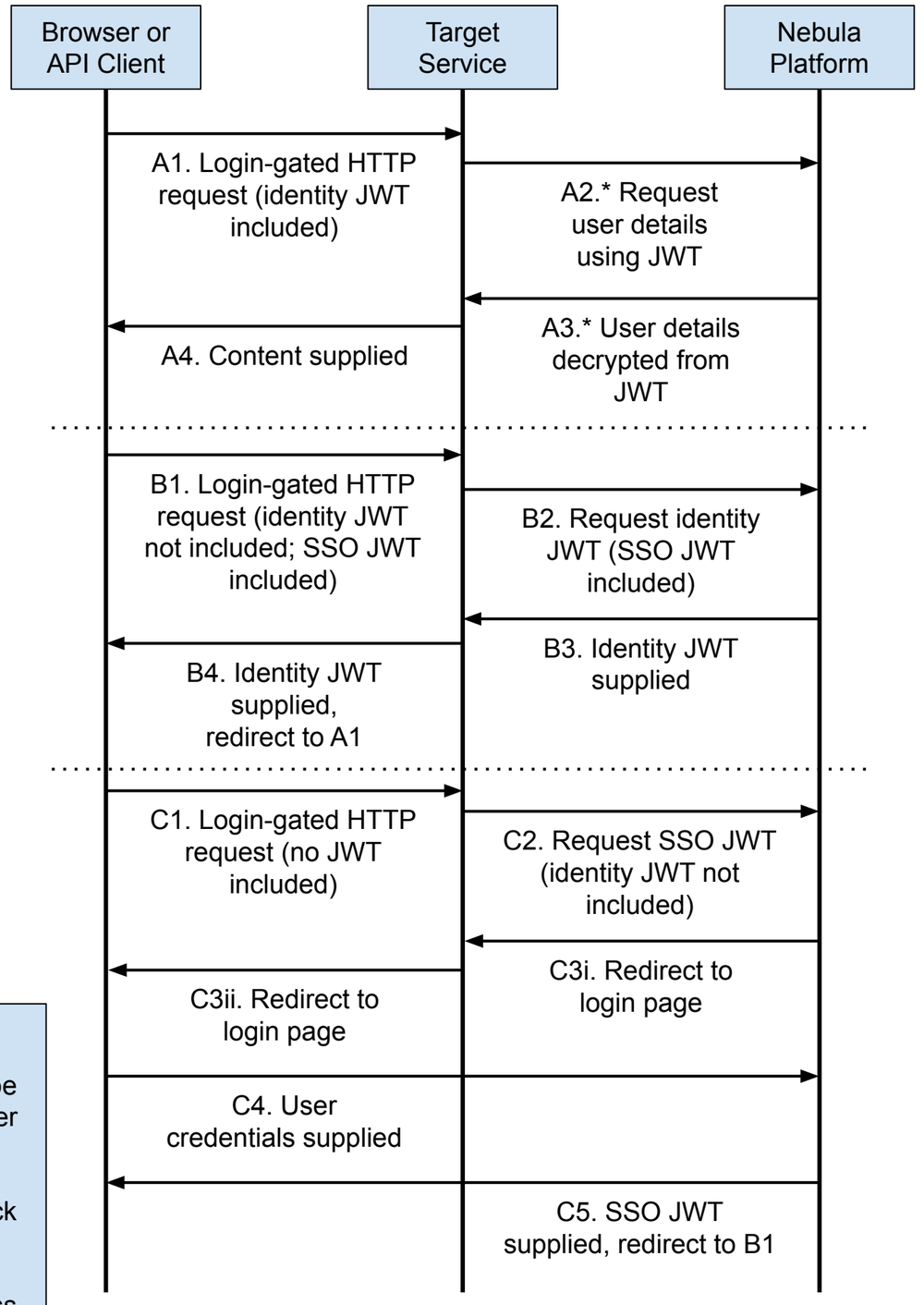
Notes (Centralized Approach)

- The auth request token contains information about the requester, e.g., the email address of the account to be used for auth and the IP address of the source machine. The auth response token indicates whether the user currently has a global session active. Both the auth request token and auth response token are digitally signed by their creators. The certificate used is exchanged during initial configuration.
- It is unclear how the destination for the redirection to (1) should be kept track of. One option is to pass it back as a query parameter in (4), then pass it as a query parameter again in (7).

Notes (Decentralized Approach)

- Redirection chains are used to ensure that the final destination URI is preserved from the start of the process to the end.
- Steps marked with * are not strictly required.
- Be very careful - data transmitted using JWTs is not encrypted, just stored in Base64Url encoding.

Decentralized Approach (Authority comes from JWT) (Good)



Sources. SSO Overview. Implementation guide (using express-session, not great). Implementation guide (using only JWTs, best). JWT overview. JWT security.