RFC 7521 token service.

Combines JWT info with out of scope

authorization logic and information and issues OAuth2 Access/Refresh token(s). Validates signature using Direct Trust Bundle containing EHRA JWT signing cert. Token service in EHRB security domain can have local communication with Resource server.

JWT Authentication Authority in Client EHRA’s security domain.

Issues signed JWT for User A. In Direct Trust Bundle with policy TBD.

User A In Client EHRA

Client EHRA

FHIR/REST API

Access on behalf of User A

Resource EHRB

EHRB server checks access token in accordance with locally implemented procedures, ensuring token has not expired, is for a correct resource (URL), and conforming with scope or other constraints relating to privacy or other security policies.