HTTP Digital Signature Algorithm (HTDSA)

Request flow diagram covering client authorization and single-sign-on scenarios.
All communication between the client application and identity provider is signed using HTDSA.

Client Browser

The user of the web service and owner of credentials on the identity provider.

Client Application

The application requesting authentication and authorization for access to account information.

Identity Provider

The server that stores and verifies user credentials and client application grants.

Request Secured Resource

HTDSA Authentication Request

HTDSA One-Time Authentication URL

307 Temporary Redirect to OTA URL

Request One-Time Authentication

User Authentication   If user is not currently authenticated (or has strict session limits), or this is the first time the user is using the app (enrollment).

Present Authentication View

User Authenticates (SRP, OTP, etc.)

Application Enrollment   If the application has not previously been granted permissions, the identity provider will confirm the user's intention.

Present Authorization View

User Authorizes Client Application

Session Negotiation   Once authentication and authorization are confirmed, the user is directed back to the client application.

303 See Other Redirect to Client Application Callback URL w/ Session Token

Request Callback URL

HTDSA Session Identity Request

HTDSA Session Identity Response

308 Permanent Redirect to Secured Resource