HEART Testing

onnect Server | Home | About | Statistics | Contact

Welcome!

OpenID Connect is an internet-scale federated identity protocol built on top of the OAuth2 authorization framework. OpenID Connect lets you log into a remote site using your identity without exposing your credentials, like a username and password.

Learn more »

bout

OpenID Connect service is built from the MITREid ect Open Source project, from The MITRE Corporation he MIT Internet Trust Consortium.

re »

Contact

For more information or support, contact the administ of this system.

Email »

urrent Statistics

ber of users: 0 Authorized clients: 0 Approved sites: 0

Eid Connect {0} .

What's this about?

From http://openid.net/wg/heart/,

> The HEART Working Group intends to harmonize and develop a set of privacy and security specifications that enable an individual to control the authorization of access to RESTful health-related data sharing APIs, and to facilitate the development of interoperable implementations of these specifications by others.

Reference implementation

According to https://bitbucket.org/openid/heart/wiki/Home,

> MITREid Connect is an open source reference implementation of OpenID Connect and OAuth 2.0 from the MITRE Corporation and MIT Internet Trust Consortium (ITC).

While MITREid Connect does not specifically mention HEART, we assume it's appearance under the "reference implementation" section of the HEART Working Group Wiki implies it supports full HEART compliance.

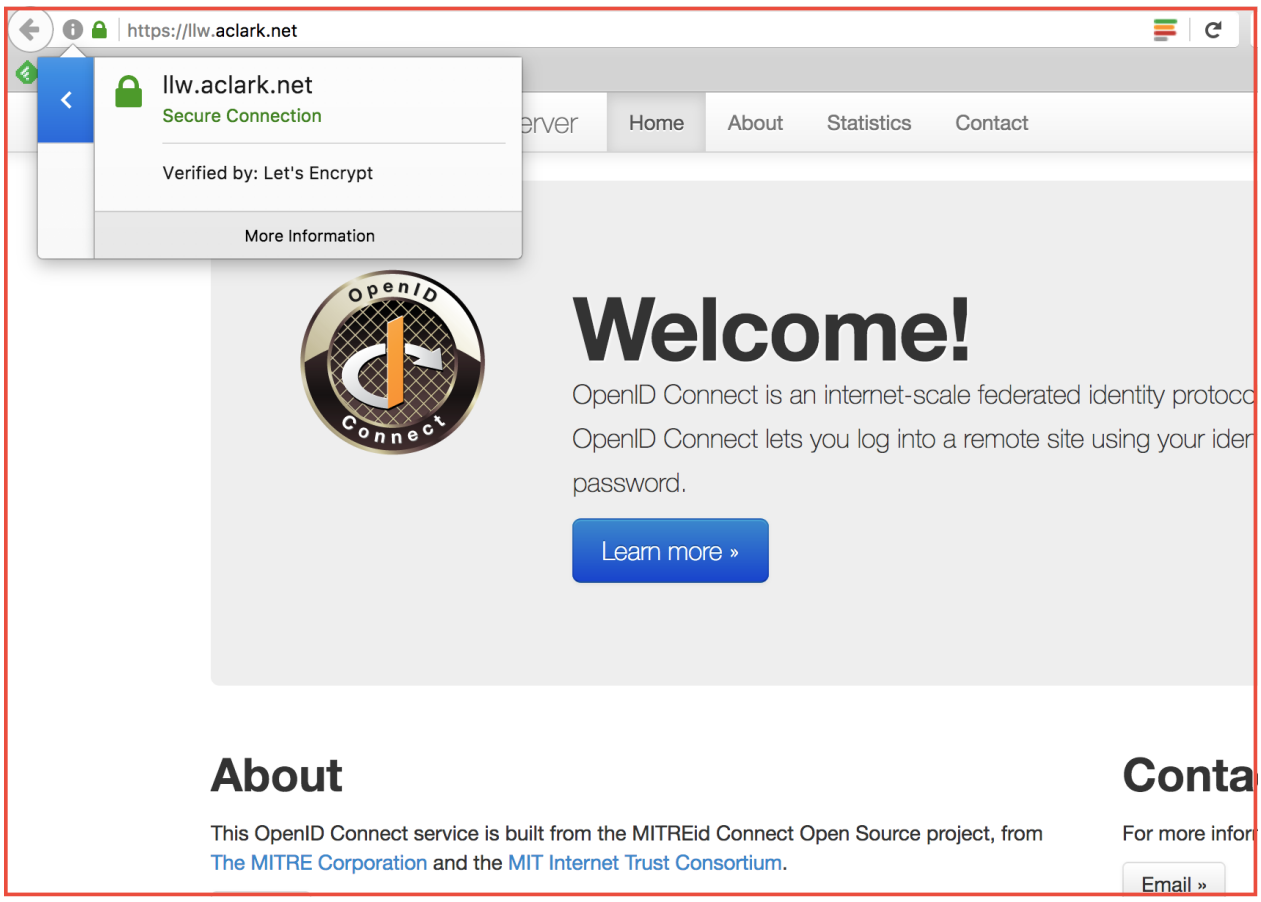
Endpoints

According to https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server/wiki/Server-configuration#endpoints, a HEART-compliant server should offer the following endpoints:

- Authorization endpoint: /authorize
- Token endpoint: /token
- Token introspection: /introspect
- Token revocation: /revoke
- JSON Web Key Set (public key): /jwk
- User info: /userinfo
- Provider configuration: /.well-known/openid-configuration

SSL

As SSL is a requirement, we have configured a free certificate from Let's Encrypt



Testing

Here we confirm our MITREid-Connect server offers the specified endpoints:

```
$ curl https://llw.aclark.net/.well-known/openid-configuration | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2829  100  2829    0     0   2540      0  0:00:01  0:00:01 --:--:--  2541
{
  "request_parameter_supported": true,
  "claims_parameter_supported": false,
  "introspection_endpoint": "https://llw.aclark.net/introspect",
  "scopes_supported": [
    "openid",
    "profile",
    "email",
    "address",
    "phone",
    "offline_access"
  ],
  "issuer": "https://llw.aclark.net/",
  "userinfo_encryption_enc_values_supported": [
    "A256CBC+HS512",
    "A256GCM",
    "A192GCM",
    "A128GCM",
    "A128CBC-HS256",
```

```
    "A192CBC-HS384",
    "A256CBC-HS512",
    "A128CBC+HS256"
  ],
  "id_token_encryption_enc_values_supported": [
    "A256CBC+HS512",
    "A256GCM",
    "A192GCM",
    "A128GCM",
    "A128CBC-HS256",
    "A192CBC-HS384",
    "A256CBC-HS512",
    "A128CBC+HS256"
  ],
  "authorization_endpoint": "https://llw.aclark.net/authorize",
  "service_documentation": "https://llw.aclark.net/about",
  "request_object_encryption_enc_values_supported": [
    "A256CBC+HS512",
    "A256GCM",
    "A192GCM",
    "A128GCM",
    "A128CBC-HS256",
    "A192CBC-HS384",
    "A256CBC-HS512",
    "A128CBC+HS256"
  ],
  "userinfo_signing_alg_values_supported": [
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
    "ES512",
    "PS256",
    "PS384",
    "PS512"
  ],
  "claims_supported": [
    "sub",
    "name",
    "preferred_username",
    "given_name",
    "family_name",
    "middle_name",
    "nickname",
    "profile",
    "picture",
    "website",
    "gender",
    "zoneinfo",
    "locale",
    "updated_at",
    "birthdate",
```

```
    "email",
    "email_verified",
    "phone_number",
    "phone_number_verified",
    "address"
  ],
  "claim_types_supported": [
    "normal"
  ],
  "op_policy_uri": "https://llw.aclark.net/about",
  "token_endpoint_auth_methods_supported": [
    "client_secret_post",
    "client_secret_basic",
    "client_secret_jwt",
    "private_key_jwt",
    "none"
  ],
  "token_endpoint": "https://llw.aclark.net/token",
  "response_types_supported": [
    "code",
    "token"
  ],
  "request_uri_parameter_supported": false,
  "userinfo_encryption_alg_values_supported": [
    "RSA-OAEP",
    "RSA-OAEP-256",
    "RSA1_5"
  ],
  "grant_types_supported": [
    "authorization_code",
    "implicit",
    "urn:ietf:params:oauth:grant-type:jwt-bearer",
    "client_credentials",
    "urn:ietf:params:oauth:grant_type:redelegate"
  ],
  "revocation_endpoint": "https://llw.aclark.net/revoke",
  "userinfo_endpoint": "https://llw.aclark.net/userinfo",
  "token_endpoint_auth_signing_alg_values_supported": [
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
    "ES512",
    "PS256",
    "PS384",
    "PS512"
  ],
  "op_tos_uri": "https://llw.aclark.net/about",
  "require_request_uri_registration": false,
  "code_challenge_methods_supported": [
    "plain",
    "S256"
```

```
  ],
  "id_token_encryption_alg_values_supported": [
    "RSA-OAEP",
    "RSA-OAEP-256",
    "RSA1_5"
  ],
  "jwks_uri": "https://llw.aclark.net/jwk",
  "subject_types_supported": [
    "public",
    "pairwise"
  ],
  "id_token_signing_alg_values_supported": [
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
    "ES512",
    "PS256",
    "PS384",
    "PS512",
    "none"
  ],
  "registration_endpoint": "https://llw.aclark.net/register",
  "request_object_signing_alg_values_supported": [
    "HS256",
    "HS384",
    "HS512",
    "RS256",
    "RS384",
    "RS512",
    "ES256",
    "ES384",
    "ES512",
    "PS256",
    "PS384",
    "PS512"
  ],
  "request_object_encryption_alg_values_supported": [
    "RSA-OAEP",
    "RSA-OAEP-256",
    "RSA1_5"
  ]
}
```