• User authentication takes place via OpenID Connect, which provides a secure way for an authentication service to confirm a successful user sign-in action to client applications.

• Client applications (e.g. HumanitarianResponse.info) sign all requests to the Node.js web services (using client IDs and secrets issued by service).

• User-to-service, user-to-client application, client application-to-service, and service-to-service connections are all encrypted using SSL.

• API keys and secrets can be expired and reissued.

• Users are protected against CSRF attacks on the authentication service using the Node.js package hapi/crumb.

• Users are protected against CSRF attacks on the HumanitarianResponse.info site and Humanitarian ID app using Drupal's form system and AngularJS's XSRF-TOKEN approach.

• Use of modern, open-source technologies with continual updates from the community to help ensure the platform remains as secure as possible.

• Users can enable Multi-Factor-Authentication as an additional layer of security.