APPENDIX 1 - eFaas

eFaas: Citizens Online Identity

National Centre for Information Technology
Ministry of Communication Science and Technology

Republic of Maldives

Vsersion: 1.3.1, Last updated on: 17-02-2019 Prepared By: MT

eFaas : Single Identity provider

eFaas is managed by the National Centre for Information Technology. We set up eFaas to make it easier for Maldivians, expatriates and organisations of Maldives to get things done online securely.

eFaas will be the de facto standard to access government and other approved digitals services online. You can use eFaas for both business and personal use. You can control what personal information is shared with the services that use eFaas.

You can verify your eFaas account using your mobile phone number and personal email address. You can also verify in-person at an authorised government office, this will ensure that your eFaas account is a government verified account.

eFaas uses industry best practices and security standards to ensure security and privacy of user data.

eFaas: OpenID Connect protocol based

OpenID Connect (OIDC) is an authentication protocol, based on the OAuth 2.0 family of specifications. It uses simple JSON Web Tokens (JWT), which you can obtain using flows conforming to the OAuth 2.0 specifications.

It is a simple identity layer built on top of the OAuth 2.0 protocol, which allows clients to verify the identity of an end user based on the authentication performed by an authorization server or identity provider (IdP), in this case eFaas, as well as to obtain basic profile information about the end user in an interoperable and REST-like manner. OpenID Connect specifies a RESTful HTTP API, using JSON as a data format.

OpenID Connect allows a range of clients, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users.

OIDC is all about user authentication. Its purpose is to give you one login for multiple sites. Each time you need to log in to a website using OIDC, you are redirected to your OpenID site where you login, and then taken back to the website.

For more technical information about the protocol: https://openid.net/connect/

eFaas: How it works

For an example signing into Application A that uses eFaas for authentication, here is how its flow works:

1. When you choose to sign in to Application A using your eFaas account, Application A sends an Authorization Request to eFaas .

2. eFaas authenticates your credentials or asks you to login if you are not already signed in, and asks for your authorization (lists all the permissions that Application A wants, for example read your email address, and asks you if you are ok with that).

3. Once you authenticate and authorize the sign in, eFaas sends an Access Token, and (if requested) an ID Token, back to Application A.

4. Application A can retrieve user information from the ID Token or use the Access Token to invoke a eFaas API.