RCL Digital Identity

The RCL Digital Identity platform allows organizations to issue Digital Identities to people. A Digital Identity is a unique representation of a person carrying out an online transaction. In this context, a person holding a Digital ID has their Personal Identifiable Information (PII) stored with an Identity Provider (IdP). This IdP will provide the functionality for the person to sign-in to various websites and transmit their PII as claims to the website. The website can then use these claims to make a determination about the user (e.g. whether to grant a service or not).

The Digital ID can be:

- Self-Asserted - independent physical identity verification of the person is not required
- Verified - the physical identity of the person is verified by a process of Identity Proofing

Self-Asserted Digital Identity

In a Self-Asserted Digital ID, the person will sign-up for a Digital ID and be immediately granted the ID once they have confirmed their email. The physical identity of the person is not independently verified. The process of granting the ID is fully automated and does not require human intervention.

Identity Self Assertion

A person will apply to the organization for a Digital Identity using an online Identity Self Assertion Application that the organization hosts. The applicant will provide their personal identification data and will verify their email address during the sign-up process. The process follows the NIST SP 800-63 IAL1 Identity Assurance level.

Verified Digital Identity

In a Verified Digital ID, the person will Enrol for a Digital ID. The physical identity of the person must be verified by an Identity Approver in an Identity Proofing process. This process requires human intervention in granting the ID.

Identity Enrolment

A person will apply to the organization for a Digital ID using an online Identity Enrolment Application that the organization hosts. The applicant will provide their personal identification data and will verify their email address during the sign-up process. The identification data will be verified by an independent Identity Approver remotely or in person. The process follows the NIST SP 800-63 IAL2 Identity Assurance level for remote verification and IAL 3 for in-person verification.

Identity Proofing

Once the applicant has completed the sign-up process, they will submit photo IDs (e.g. National IDs, Drivers Permits, Passports) to verify their personal identification. An Identity Approver will review the photos and approve the Digital ID when the applicant's identity is physically verified. Identity proofing is carried out by the approver in the issuing organization using an online Identity Proofing Application hosted by the organization.

Digital ID

The person's Digital ID data will be managed in Azure Active Directory B2C (AAD B2C) acting as an Identity Provider (IdP). The organization will subscribe for and control the AAD B2C tenant in their Azure subscription. The following User Claims are stored and issued by the IdP:

- Given Name
- Surname
- Display Name
- Street Address
- City
- State/Province
- Postal Code
- Country
- Email
- Object Id

Additional claims for a Verified Digital ID

- Date of Birth
- Identity Approver

The unique identifier for the person's Digital ID will be stored in the Object Id.

Single Sign-On

A person with a Digital Identity will utilize Single Sign-On provided by the AAD B2C IdP to sign in to multiple web sites using the same sign-in credentials.

Single Sign-On is compliant with the Open ID specification. Using Open ID, the Digital ID issuing organization can set up single sign-on on multiple regional and international websites it directly controls.

It can also allow its partners and external organizations (Relying Parties) to use its AAD B2C as an External Identity Provider (External IdP) to sign in its users to external websites using the Authorized Code Grant type described in the OAuth2 specification.

Authentication

The Digital ID issuing organization can set up single-factor authentication using username and password credentials. This follows NIST SP 800-63 AAL1 Authenticator Assurance level.

In addition, multi-factor authentication utilizing the time-based one-time password (TOTP) verification process is supported. This is done using an Authenticator Application (e.g.: Google Authenticator, Microsoft Authenticator). This follows NIST SP 800-63 AAL2 Authenticator Assurance level.

User Claims

The AAD B2C Identity Provider will send the User Claims in the JWT tokens when a user signs in to a website. Using these claims, the relying parties to which the person signs in will have access to the Personally Identifiable Information (PII). The relying party will use the PII to make decisions about the user (e.g. whether to grant a service).

Standards Compliance

The RCL Identity platform are APIs built on Azure AD B2C and is compliant with the following standards:

- NIST SP 800-63 Digital Identity Guidelines
- OAuth2 Authorization Framework for single sign-on
- Open ID for single sign-on
- SAML for single sign-on

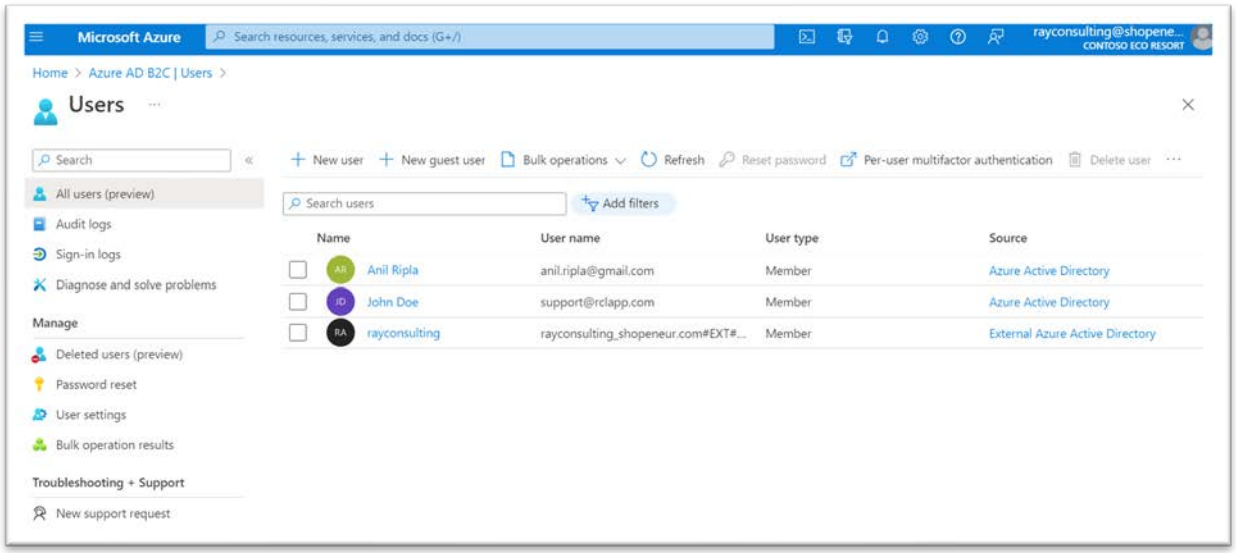
Architecture and Applications

Cloud Services

The organization issuing the Digital ID will subscribe for the applicable cloud services provided by the Microsoft Azure Cloud. The organization will have sole and full control over its cloud services and resources.

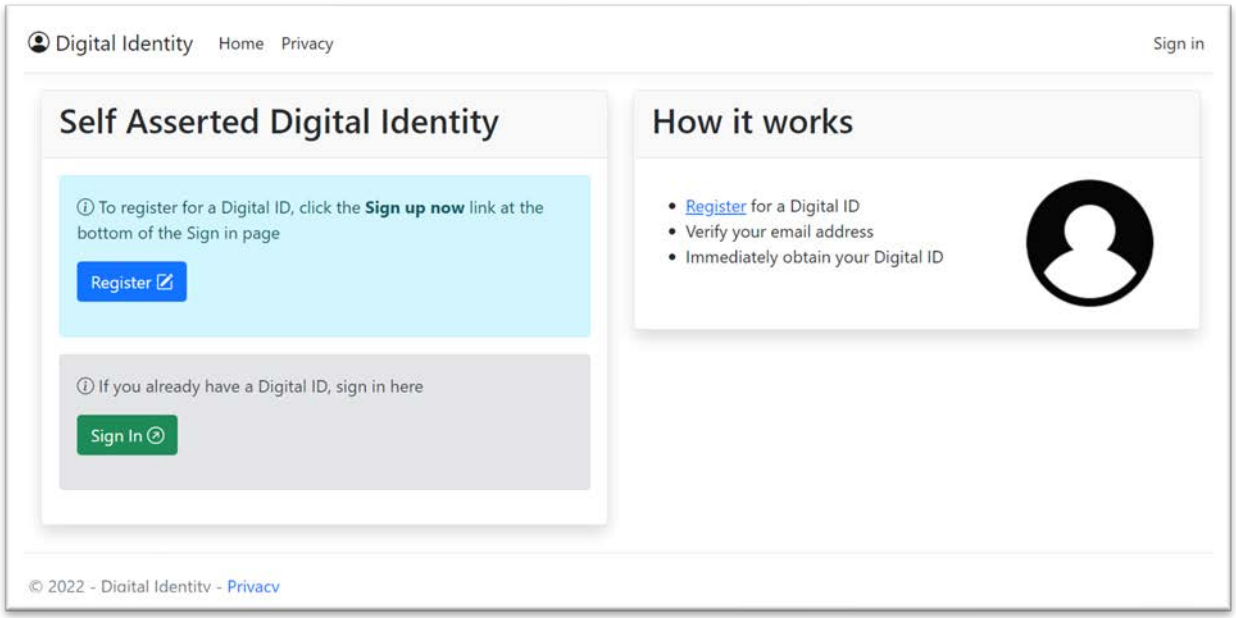
Azure AD B2C

The organization will create and administer an Azure AD B2C tenant that will act as an Identity Provider (IdP) and will use it to store identity data for those people that they issue Digital IDs. The IdP will also provide single sign-on technology using OAuth2, SAML and OpenID. The organization will have sole and full control over its IdP.



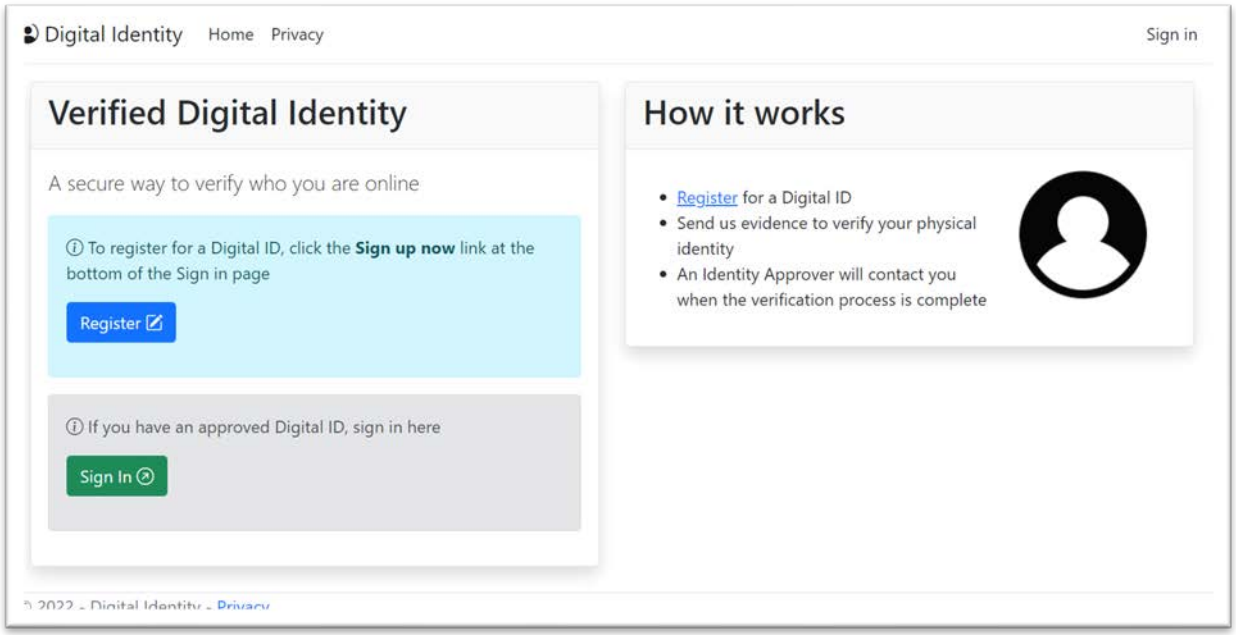
Identity Self Assertion Application

For a Self-Asserted Digital Identity, the organization will host the open-source Identity Self Assertion Application as a Web App in its Azure subscription. It will have full control over this application.



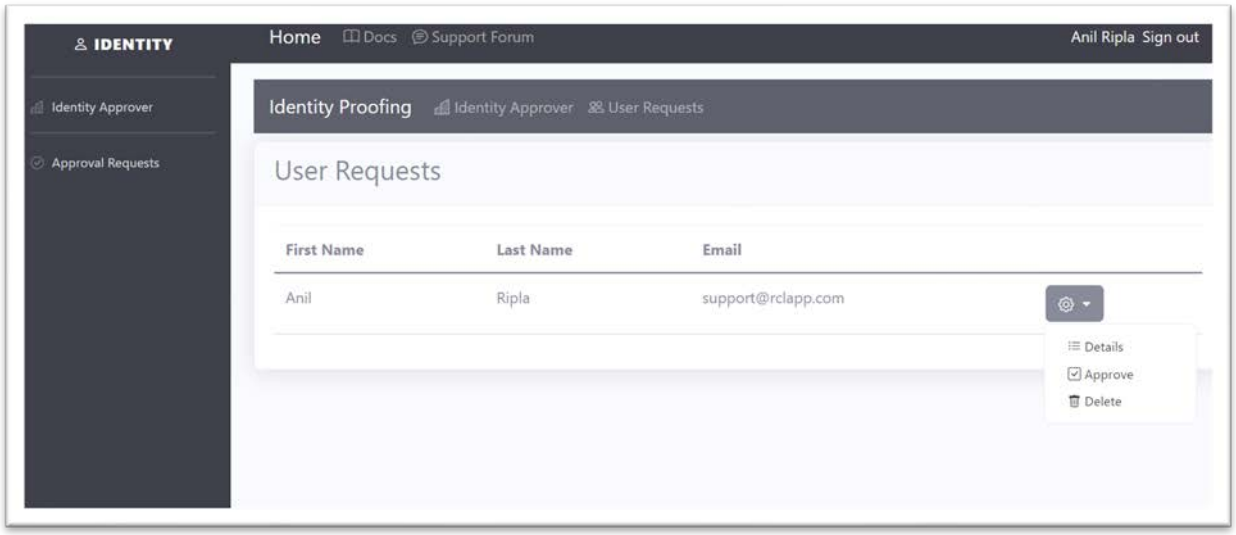
Identity Enrolment Application

For a Verified Digital Identity, the organization will host the open-source Identity Enrolment Application as a Web App in its Azure subscription. It will have full control over this application.



Identity Proofing

For a Verified Digital Identity, the organization will host the open-source Identity Proofing Application as a Web App in its Azure subscription. It will have full control over this application.



RCL Identity SaaS application

For a Verified Digital Identity, the organization will subscribe to the RCL Identity Software as a Service (SaaS) application provided in the Azure Marketplace to access the RCL Identity Platform APIs to facilitate Identity Proofing. The organization will have full control over this application.