
EcoRegistry.

Content

Who we are

EcoRegistry is a software-based company that aims to support sustainable development initiatives through technological solutions. Our founding team recognized the need for an information management system for sustainable development and the importance of transparent results in tackling climate change. As a result, we developed a registry system for Carbon crediting programs that track the information supporting each carbon credit, its origin, and its beneficiary.

Our platform offers services to Carbon offsetting standards, countries for NDC registry systems, and other organizations that need to register climate assets. We prioritize connectivity between multiple platforms to facilitate information exchange and transparency. Our accounting system provides easy access to verifiable information, ensuring the integrity of all transactions and no double counting of climate asset transactions; it also utilizes the virtues of a blockchain system implemented on a virtual private network. Transparency and traceability are crucial to building trust in the climate asset market.

At EcoRegistry, we are constantly developing and implementing new technologies to improve our platform. For example, we are currently working on digitized MRV solutions, system control/risk management, and automated reports and information for end users. Our goal is to bring the newest technology and tested systems to the service of the people.

Our platform design is based on three core pillars: **simplicity** and **agility**, **connectivity**, and **transparency**. Our system must always be simple and agile to offer project developers flexibility. It must also provide simple access to all the information supporting each climate asset to ensure informed decision-making. Connectivity is a crucial aspect of our platform, allowing for easy information exchange and implementing new sustainable development initiatives. Finally, we provide transparent information and traceability of all projects and climate assets to promote integrity and trust.

Purpose of this document and intellectual property rights

The purpose of this document is to provide information on EcoRegistry's official document publication and intellectual property rights. Furthermore, the official record is intended for public use and contribution to developing a robust ecosystem and will always be available on our website, www.ecoregistry.io.

At EcoRegistry, we achieved integrity and trust by sharing information and contributing to the ecosystem from all perspectives. Therefore, this document represents our proposal to establish a worldwide information exchange system, allowing anyone around the globe to access information about sustainable development projects.

For further information or inquiries, please do not hesitate to contact us through our website or email at contacto@ecoregistry.io. We welcome feedback and suggestions for improving our platform and services. Additionally, please note that this document's intellectual property rights and copyrights belong to EcoRegistry. Therefore, the unauthorized use or reproduction of this document is strictly prohibited.

We hope this document is valuable to you, your team, your company, and your country. Please feel free to use it as a resource, and we welcome your contributions to the development of a sustainable future.

Introduction

The Paris Agreement is a legally binding international treaty with the participation of over 190 countries, aimed at reducing greenhouse gas emissions and limiting global temperature increases to below 1.5°C. In addition, the Parties are expected to submit their Nationally Determined Contributions (NDCs) as a roadmap to address climate change and build resilience in their territories.

Implementing the Paris Agreement requires the development of registry systems that can track emissions, reduce, and avoid greenhouse gas emissions. In particular, Article 6 of the Paris Agreement provides insights into fostering cooperative, market, and non-market approaches to achieve mitigation targets. However, one of the most significant challenges in implementing Article 6 is the avoidance of double-counting carbon emissions, which carbon credit registries must address to ensure trust in buyers.

At EcoRegistry, we recognize the importance of connectivity and information exchange to support decision-making for a climate-positive future. As a technology solutions provider, we are committed to developing innovative solutions that promote and accelerate the implementation of climate-positive activities and projects. To this end, we have developed a registry system that adheres to our core principles of transparency, trust, and agility while constantly evolving to meet the needs of our planet. In this document, we will explain our database model and interfaces that facilitate the exchange of information required for implementing the Paris Agreement and achieving climate-positive outcomes.

When creating a software system, it's essential to consider many different factors that contribute to its overall quality, such as how fast it can perform, how well it can handle increased usage, how secure it is, and how easy it is to make changes to or maintain over time. To address these concerns early in the development process, architects create high-level structures that help guide the system's design and development, ensuring that these quality attributes are considered from the beginning and throughout the system's life cycle.

Our Principles

We understand the importance of transparency, technological advancement, connectivity, integrity, availability, and confidentiality in governing our operations at EcoRegistry. These principles have been established by EcoRegistry to ensure compliance with international information management standards such as ISO 27001 and to promote trust among all stakeholders.

Transparency

Transparency is a fundamental principle that guides our operations. We provide genuine, precise, appropriate, sufficient, and auditable information about all projects and participants on the platform. This principle ensures that stakeholders clearly understand all information displayed on EcoRegistry, and they can contact us for details. EcoRegistry must provide transparent and traceable project data to promote integrity and trust in the climate asset markets.

Technological vanguard

At EcoRegistry, we are committed to remaining at the forefront of technological advancements that support sustainable development initiatives. Our team is constantly developing new solutions to meet the needs of our customers, and our system is continuously evolving. While our primary focus is currently on registry systems, we are open to adapting to any other solution that meets the market's changing needs.

Connectivity

Connectivity worldwide is essential to scale solutions and promote trust and reliability in the system. We believe in connecting all groups of interest to enhance the quality of our platform through feedback. This way, users can access information about sustainable development initiatives, analyze market behavior, and apply the required data analytics to enhance the quality constantly through feedback from the groups of interest.

Integrity

Integrity is vital in promoting trust over the life cycle of each implementation. Therefore, we ensure that all data about projects and activities is always consistent, providing accurate information that supports a positive climate impact and avoiding any unwanted changes to this information.

Availability

EcoRegistry prioritizes the availability of authorized parties to access the information required at any time and from anywhere worldwide. Therefore, the technical infrastructure and the display of this information must always be in place so that all have proper access to it.

Confidentiality

At EcoRegistry, the confidentiality of our users and clients is of utmost importance to us. Therefore, we take great care to categorize databased on its level of sensitivity and implement strict measures to prevent unauthorized access, disclosure, or use of the data.

Our commitment to data confidentiality is crucial to our mission to provide a secure and trustworthy marketplace for climate asset trading.

We understand that our users and clients rely on us to protect their confidential information, and we take that responsibility very seriously. Our security protocols and encryption methods are designed to safeguard our users' data from potential cyber threats. At the same time, we ensure that all of our employees are well-versed in data protection and confidentiality practices.

Architecture

EcoRegistry is a software-based company that provides technological solutions to support sustainable development initiatives. The company's platform offers services related to offsetting carbon standards and NDC (Nationally Determined Contribution) registry systems for countries and other organizations that must register climate assets.

Application Architecture

EcoRegistry's technological architecture has been designed as a comprehensive cloud-based solution, integrating various cloud services to optimize performance and functionality. The platform is deployed on Amazon Web Services (AWS), utilizing a range of services, including Elastic Beanstalk for automatic scaling and high availability, Lambda for serverless computing, and CloudFront for content delivery. This combination of services provides a scalable and highly available architecture capable of handling large traffic volumes while maintaining high performance and reliability. Additionally, the platform leverages cloud-based databases for efficient data management and storage while integrating with third-party APIs and services to expand its functionality and capabilities. The content delivery network (CDN) is built using the Amazon CloudFront service and is integrated with the back-end services to optimize content delivery and improve user performance. Each user will access our platform through our server-client interaction modules using an HTTPS-secured connection according to security standards.

The system's front-end consists of a multipage interface and employs HTML, CSS, and JavaScript, along with React and Bootstrap, to enhance usability and streamline development. The back-end uses the Express framework, which provides a scalable and flexible server-side architecture. In addition, a RESTful API facilitates communication between the front-end and core back-end, which enables data exchange and supports various business processes.

The platform features a georeferencing service that analyzes project overlap. This service is deployed serverless, using the Python runtime environment, and it integrates with the

primary system via an API Gateway that provides a RESTful interface for communication with the back-end.

EcoRegistry relies on two types of databases to manage and secure its data. First, a relational database that stores customer information, project data, and order details. This type of database allows for efficient data storage and retrieval, data integrity, and scalability. Additionally, EcoRegistry has implemented a blockchain-based database to safeguard the issuance and transaction history of assets within the system. The core back-end communicates with an API that interacts with the blockchain, ensuring that data is securely and transparently stored and managed. This integration with blockchain technology enhances the security and reliability of the system by providing the integrity and immutability of the data stored within the system. By employing these three-layer implementation (Business layer, a Data layer, and a Blockchain information layer), EcoRegistry can ensure that its data is efficiently managed and protected, providing customers with the confidence and assurance that their information is safe and secure.

Infrastructure Architecture

This section describes the architecture of a full-stack web application built using a combination of managed and self-managed services on the Amazon Web Services (AWS) platform. The architecture follows the Model-View-Controller (MVC) pattern and uses React for the front end, Node.js for the backend, MariaDB for the central database, blockchain for transaction data, and a serverless service for georeferencing.

Architecture Overview:

The application consists of the following components:

Front-end: The front-end of the application consists of two separate applications, one for user interface and the other for administration. Both front-ends are built using React and deployed on different S3 buckets. The front ends allow users and administrators to interact with the application and provide an intuitive user interface.

Backend: The backend of the application consists of two separate applications, one for user interface and the other for administration. Both backends of the application are built using Node.js and follow the MVC architecture. The backends are deployed on separate NGINX servers on Elastic Beanstalk, allowing you to manage the infrastructure and scalability of each backend independently. In addition, the backends communicate with the same database using the MySQL protocol.

Blockchain: Blockchain technology stores transactional data, providing a secure and immutable record of all transactions in the application. The implementation is made through an independent network that enables us to manage and control de blockchain system, and

this technology allows us to use colored coins as our differentiator for each token that we generate.

Other Services: A serverless service is used for georeferencing, allowing the application to perform this task without managing any infrastructure.

Technical Details:

Front-end: The React-based front-ends are built as a static website and deployed on separate S3 buckets. The users component is served using Amazon CloudFront, which provides users worldwide with low-latency access to the application.

Backend: The NodeJs-based backend follows the MVC architecture, with the NGINX server on Elastic Beanstalk managing the infrastructure and scalability. The backend communicates with the MariaDB database using the MySQL protocol. The database is deployed on Amazon RDS, which provides easy management, security, and scaling of the database.

Blockchain: The blockchain component running on EC2 service provided by AWS. The application communicates with the blockchain using the Multichain protocol and stores transactional data in the blockchain. The Python-based API for the Blockchain runs with the NGINX server on Elastic Beanstalk.

Other Services: The serverless component uses AWS Lambda and API Gateway. The Lambda function performs the georeferencing task and is triggered by API Gateway.

Network and security architecture

The network architecture for the web application is designed to provide a secure and scalable environment for the application to operate in. The architecture includes the following components:

Amazon VPC: The application deployed within an Amazon Virtual Private Cloud (VPC) provides a private network infrastructure for the application to operate within. The VPC is logically isolated from other resources within the AWS cloud, providing an additional layer of security.

Subnets: Within the VPC, the application is deployed across multiple subnets, each located in different Availability Zones (AZs), ensuring that the application can continue to operate even in the event of an AZ outage.

Elastic Load Balancer: The Elastic Load Balancer (ELB) is used to distribute incoming traffic to the application across multiple backend instances, providing a scalable solution for handling varying traffic levels.

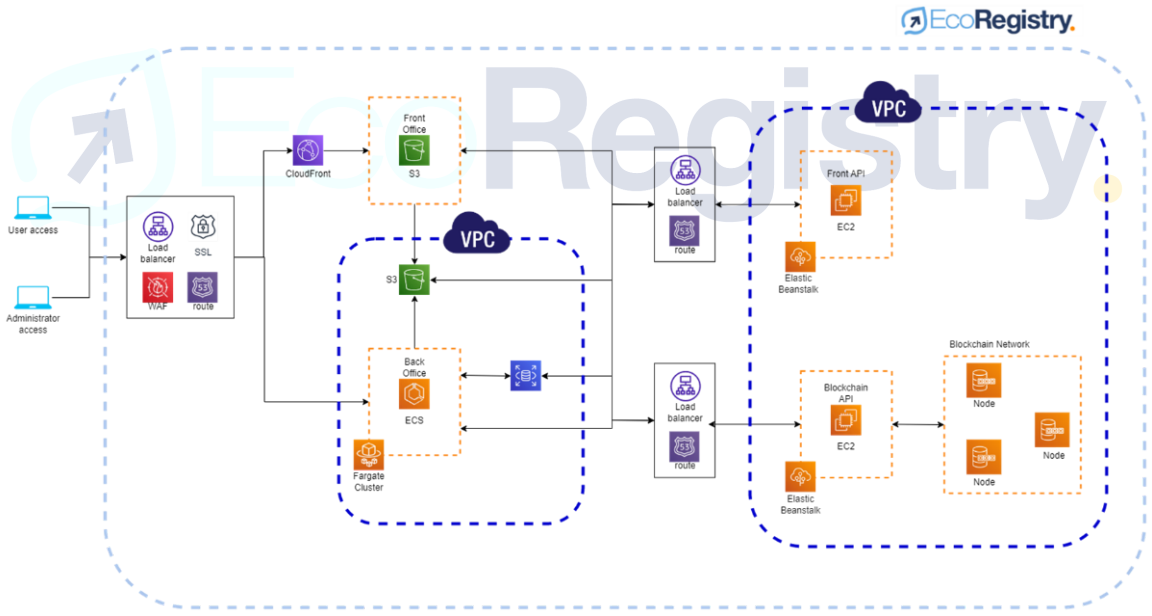
Security Groups: Security groups are used to control access to the application resources. Each resource within the application is assigned a security group, which defines the inbound and outbound traffic allowed to access the resource.

The security architecture for the web application is designed to protect the application from potential security threats. The architecture includes the following components:

Amazon IAM: Identity and Access Management (IAM) is used to manage user access to the AWS resources that the application utilizes. IAM allows for fine-grained control over user permissions, ensuring users only have access to necessary resources.

SSL/TLS Certificates: SSL/TLS certificates are used to encrypt traffic between the application and its users, ensuring that any sensitive data is protected in transit.

Web Application Firewall (WAF): The WAF protects the application from common web-based attacks such as SQL injection, cross-site scripting, and others. The WAF is configured with rules that block known attack patterns, providing an additional layer of security.



Integration and Interoperability Architecture

Description of the company's approach to integrating systems and data across the enterprise

EcoRegistry's approach to integrating systems and data across the enterprise is based on the principles of service-oriented architecture (SOA) and microservices architecture. This approach enables the company to achieve loose coupling, which facilitates agility and flexibility in the integration of systems and data. Additionally, EcoRegistry's approach emphasizes the use of APIs and web services to provide a standardized interface for system

and data integration, allowing for interoperability and communication between different systems.

Standards and protocols for integration and interoperability

EcoRegistry implements the highest security and reliability standards to ensure secure data exchange. Our services on the cloud comply with the NIST 800-53 framework, with shared responsibility between our team and the cloud provider to ensure secure data management. The platform uses secured communication standards such as SSL/TLS in its latest versions to comply with ISO/IEC 27017 and other ISO 27000 family standards, particularly ISO 27001. EcoRegistry's implementation of ISO 27001 and its enhanced principles ensure confidentiality, availability, integrity, connectivity, and transparency at any time.

To prevent non-secure connections and potential attack attempts from the outside, EcoRegistry has installed a Web Application Firewall (WAF). For the specific connectivity to other platforms, EcoRegistry provides a web service that includes an authentication protocol with a token valid for one hour, as the best practices of OWASP (Open Web Application Security Project) suggest.

Transactions are used either through REST (Representational State Transfer) or SOAP (Simple Object Access Protocol) communication protocol using encrypted channel to ensure secure data transfer. The implementation of SOAP is based on an XML (Extensible Markup Language) and the REST implementation is based on JavaScript Object Notation to ensure the correct definition of data objects and values according to the specified structure. EcoRegistry has implemented continuous hacking to look for any vulnerabilities before deployment.

Architecture patterns for achieving integration and interoperability

EcoRegistry employs several architecture patterns to achieve integration and interoperability across its systems and data. These include the ESB (Enterprise Service Bus) pattern, which facilitates communication and data exchange between different systems through a centralized hub. The company also uses the event-driven architecture pattern, which allows for real-time communication and data exchange between different systems and applications. Additionally, EcoRegistry utilizes the microservices architecture pattern, which facilitates the development of independent, loosely coupled services that can be easily integrated and scaled as needed.

Security

EcoRegistry has implemented various security measures to ensure the confidentiality, integrity, and availability of data stored and processed within the platform. The following sections describe the security measures in place:

Data Transfer Security:

EcoRegistry employs a secure web application firewall (WAF) to ensure reliable network and API data transfers. All data transfer between users and the platform is encrypted using SSL/TLS. EcoRegistry uses AES-256 encryption to safeguard all information stored in encrypted databases, both at rest and in transit.

Cloud Security:

EcoRegistry's software architecture is based on Amazon Web Services (AWS) cloud platform, which implements robust security standards and technologies. All cloud components and services used in the IT ecosystem are private by design, and communication between them occurs over a private network. The communication between all the components and services has appropriate security mechanisms in place, such as firewalls, Security Groups, NACLs, and Virtual Private Cloud.

Access Control and User Management:

Access to the registry is granted exclusively through the secure online platform, which uses multi-factor authentication to protect against unauthorized access. EcoRegistry has implemented a robust user management system that allows creating and administering distinct access levels to the platform. EcoRegistry provides various user types with specific permissions and an independent view of the platform upon access.

Distributed Ledger Technology:

The information is safeguarded under encrypted databases through a Distributed Ledger Technology (DLT). The EcoRegistry's blockchain-based solution has been granted an EBSS (Enterprise Blockchain Security Specification) compliance according to an audit processed by S2 Group. The DLT characteristics correspond to the decentralization of data, validation of transactions by peers, registered information immutability, and implementation of consensus mechanisms.

OTP Authentication:

EcoRegistry ensures that no action is performed on the platform without the activation of commands executed by the user. During any transaction or project state change, the platform provides a dynamically created OTP (One Time Password) to the user. The OTP is

sent through email or SMS, requiring the user to confirm the process before completing any action.

Intrusion Detection/Prevention:

EcoRegistry is continuously assessing and improving its security posture by conducting ethical hacking activities. The company's technical team performs regular security assessments and penetration testing to identify and address potential vulnerabilities in the platform. Additionally, EcoRegistry partners with third-party security firms to conduct independent audits and assessments to ensure that the platform meets the highest security standards.