
## A Platform Approach to

# Delivering Decentralized Identity Service Offerings

The Anonyome Labs platform includes a comprehensive Decentralized Identity service offering using a cloud-based, SaaS deployment model. Using this approach, Anonyome provides a complete and managed solution that includes: the deployment, management, maintenance, and support of its Decentralized Identity services. This allows customers to focus on their core businesses while leaving the detailed technical operations work to Anonyome.

This also gives customers a faster deployment of Decentralized Identity capabilities and a massive reduction in the Total Cost of Ownership (TCO) compared to other deployment models.

SUDO PLATFORM

# Introduction

For software providers and integrators, adding a Decentralized Identity infrastructure to their product lines introduces many of the same choices they faced when integrating other system elements. For example, some companies choose to host their webservers in their own local data center using their own hardware, while many opt for the simplicity of leasing server space from a cloud hosting provider. Both methods have benefits.  Some companies enjoy the peace of mind that comes with controlling their own hardware and software stacks. For others (an increasing majority), peace of mind comes from knowing that the hardware and software stacks are delivered and maintained through a contract model. The latter is often referred to as  cloud hosting or the more formal Software as a Service (SaaS) model, is widely used, because the outsourced provider deploys, manages, maintains, and provides support for the software.

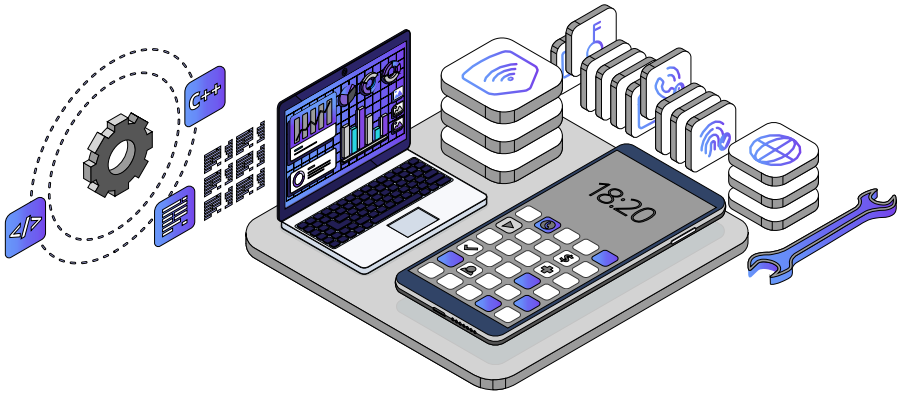
The decision of whether to use a SaaS or on-site deployment model is usually determined by calculating the Total Cost of Ownership (TCO). The key cost drivers for any software implementation are the cost of the software application, hardware / hosting costs, and costs related to staff required to deploy, manage, maintain, and support the application.  Any of those cost drivers that can be successfully outsourced become line items in a budget without the operational complexities imposed by on-site deployments. Other organizations may choose to operate and manage a deployment through a third-party cloud hosting provider
Many companies have calculated the inefficiency, complexity, and the additional expenses of the traditional on-site software model and have opted for the simplicity of SaaS models. The following sections describe why the SaaS model has become the de facto standard for delivering software solutions and why the Anonyome Platform has been built to embrace this model.


## No Upfront Capital Costs

The first advantage of the SaaS model is that a customer does not have to bear the upfront capital costs of deploying a software solution or even contracting for their own cloud provider. In a SaaS model, these costs (e.g., hardware / hosting, software application, and IT staff hiring / training) are incurred by the SaaS provider vendor. This simplifies initial deployment and operating costs for customers who only pay a monthly or annual subscription cost, which immediately provides benefits in terms of immediate deployment and a more friendly line item on the balance sheet.

## Speed of Deployment

Another critical advantage of the SaaS model is the speed by which a software solution can be available for customers to use. With SaaS, application software is available almost instantly to the customer. This is a far more attractive option when compared to the many months typically required for deploying and testing in-house solutions. Anonyome provides a fully automated approach to deploying new environments for customers.




## Maintenance/Upgrade of Software

In the on-site solution, a customer must ensure that the application software is updated, the operating systems are kept up to date, and any security patches are applied in a timely fashion. Additionally, customers must perform a series of compatibility tests with every change. Alternatively, in a SaaS model, the software provider ensures that the software stack is always maintained and upgraded for the customer. This includes delivering new versions of the application software and ensuring that any hosted systems are also suitably patched to protect against security vulnerabilities or deploy the latest updates on an ongoing basis as part of a service level agreement (SLA).

## Staffing Skills

The personnel required to research, design, integrate, test, fine tune, and launch any system is a significant upfront cost associated when deploying in-house solutions. Some estimates show that staffing costs account for up to 75% of the overall costs of an in-house deployment model. Alternatively, the SaaS model eliminates the staffing concerns for in-house or contracted services, where necessary resources are simply part of the SaaS subscription.

In new emerging areas such as Decentralized Identity, it also may be difficult to find people to hire who already have the requisite technical skills. Anonyome Labs has many years of experience with Decentralized Identity technologies and maintains an experienced staff that are well-versed in DI technologies. The Anonyome staff goes beyond leveraging their expertise to build the Anonyome Platform, but also actively gives back to the industry by participating in and contributing to the Decentralized Identity standards organizations that create the DI standards, which serve to increase privacy, security, and interoperability for all DI products.

## Application Scalability

With in-house solutions, customers must focus on the intricacies of infrastructure issues such as network bandwidth, database and server sizing before considering whether to ramp up their solutions. The customer using a SaaS deployment model does not have to concern themselves with the technical how of scalability, because this has already been done for them. This leaves SaaS customers free to focus on their business strategy and when to scale so as to best increase revenues.

## Software Support

The Service Level Agreement (SLA) is an important aspect of the software solution and one of the key advantages of SaaS. This agreement provides the customer with reliable actions and response times should any platform issues arise. Anonyome's global workforce ensures that priority issues are handled by staff located across multiple time zones and that responses are made … even when it is after hours at the customer's site.

## High Level of Security and Privacy

On today's internet, security and privacy are continuously moving targets. It is a very challenging task to keep application software at a consistently high-level of security and privacy protection for customer data. Customers who undertake this alone must develop a high level of proficiency and hire employees with the best security/privacy skills. Alternatively, under a SaaS deployment model, the software provider focuses on hiring and training employees in order to maintain top security and privacy skills and capabilities on behalf of the customer.

# Decentralized Identity

Decentralized Identity (DI) is major step forward in the advancement of identity management.  DI is designed to provide greater security and data privacy and is rapidly becoming an integral part of many industries where legacy centralized identity models are no longer sufficient. Legacy centralized identity models are becoming routinely exploited whether it is by rogue operators within the enterprise itself, or by third parties leveraging the unnecessary sharing of data, or through other means of gaining unauthorized access to the data.

The focus of Decentralized Identity is to eliminate many of the problems of centralized models, such as:

- **Safer:** removing the centralized management element common in today's identity and access management, there is a reduced risk of credential theft, since credentials are not centrally stored.
- **Reduced Risk:** reduces operational risk for organizations as the custodian of sensitive data. Relieves organizations of the need to repeatedly collect and distribute data.
- **Individual Control:** improves the customer/user experience by placing them in control of their data and unifying their experiences.
- **Faster:** accelerates the sign-up and sign-in process by removing the need to duplicate efforts and approvals.
- **Compliance:** facilitates easier compliance by eliminating manual error and inconsistent and redundant data distribution and validation.


**Another objective of the SaaS deployment model of the Anonyome Decentralized Identity services is to allow any customer to very quickly deploy these capabilities to their application environment. Additionally, since the deployment, management, maintenance and support is provided by Anonyome Labs,  customers no longer need to become a technical expert in this area and can focus on high-level strategy issues.**

Within the Decentralized Identity offering, the Anonyome Platform provides several licensable products:

**White Label Mobile DI Wallet:**

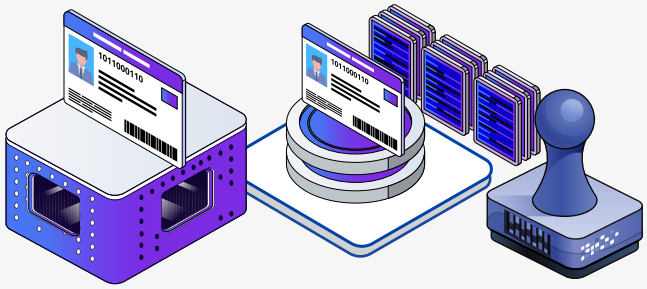
A standalone mobile application for iOS and Android, the mobile DI wallet can be used by a user for DI interactions and storage: creation and storage of cryptographic keys, the creation of connections for receiving, holding and presenting verifiable credentials. It interacts with Verifiable Credential Issuers and Verifiers. The DI wallet supports both AnonCreds and W3C Credential formats.


**Mobile Native DI Wallet SDK:**

For customers that want to add the DI Wallet functionality to their own mobile application, this native mobile SDK provides the capability for storage, cryptographic key creation, connection establishment and for receiving, holding and presenting verifiable credentials.


**Verifiable Credentials Service/SDK/Sample Apps:**

This service provides the ability to establish connections with DI Wallets and to issue verifiable credentials. It also provides the ability to request and verify presentation proofs from DI Wallets. The Verifiable Credentials Services supports both AnonCreds and W3C Credential formats.

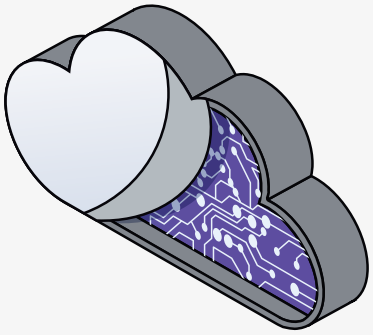


**Relay Service/SDK:**

Introduces an always-on capability for a mobile DI Wallet. Implemented as a cloud service, the Relay Service provides mediator capability for incoming/outgoing Verifiable Credential and other messages, so that sending and receiving is not limited to when the client implementations of the mobile DI Wallet and SDK are online.


**Governance framework:**

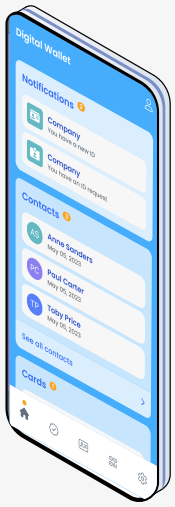
empowers DI network participants to enforce rules while staying true to the tenants of Decentralized Identity. Organizations can define and enforce governance rules associated with their ecosystem including which wallets, issuers, and verifiers are trusted and which credentials are allowed to be used and requested.



In addition to the current Anonyome DI products, the following product is also under development:

**Enterprise DI Wallet:**

A combination mobile wallet application and cloud wallet, the Enterprise DI Wallet is aimed at providing a wallet for an enterprise that is usable by multiple wallet administrators and manages credentials associated with the enterprise. Differing from a Personal DI Wallet, the Enterprise DI Wallet is intended to be used by one or more users simultaneously while also being inheritable by a future occupant of a particular job or position within an Enterprise.



# The Anonyome Platform Approach

The Anonyome Labs platform is delivered using a SaaS model. Known as the Sudo Platform, it provides a set of cybersecurity, privacy and Decentralized Identity services and SDKs that enable application developers to add these capabilities to their own applications.

When a customer has licensed one or more of the Sudo Platform services, a new Sudo Platform deployment instance is created for that customer that contains their specific licensed services. A unique feature of the Sudo Platform is that rather than take a shared deployment model (as is common for SaaS environments), the Sudo Platform deploys environments individually for each customer allowing the customer to customize the environment for their needs and it provides complete separation of data and processing from other customers.

Once an environment is deployed and configured for a customer, it is then the responsibility of Anonyome Labs to maintain and support this environment. This includes providing updates to the Anonyome Services, providing any software patches to the environment, and monitoring the environment 24x7.

## Fast Automated Deployment

Anonyome Labs has an “infrastructure as code” approach to deploying services. All licensed services are automatically provisioned to a new environment through a simple configuration process performed by Anonyome Labs. Each environment deployed is solely for use by the specific customer as a dedicated, hosted platform service.

Figure 1 (below) shows a single development environment set up for using the Decentralized Identity mobile wallet. The wallet itself is deployed from the AppStore or Playstore (alternatively apps being tested are deployed from AppTester or TestFlight). Anonyome provides a white label Decentralized Identity wallet that can be easily customized to match the branding of the customer.

The accompanying Decentralized Identity relay is deployed into the customer’s environment as an always-on mediation endpoint for the wallet. That way no matter whether the wallet is on and connected to a network, the relay can receive messages on behalf of the wallet and forward when the wallet comes back online.

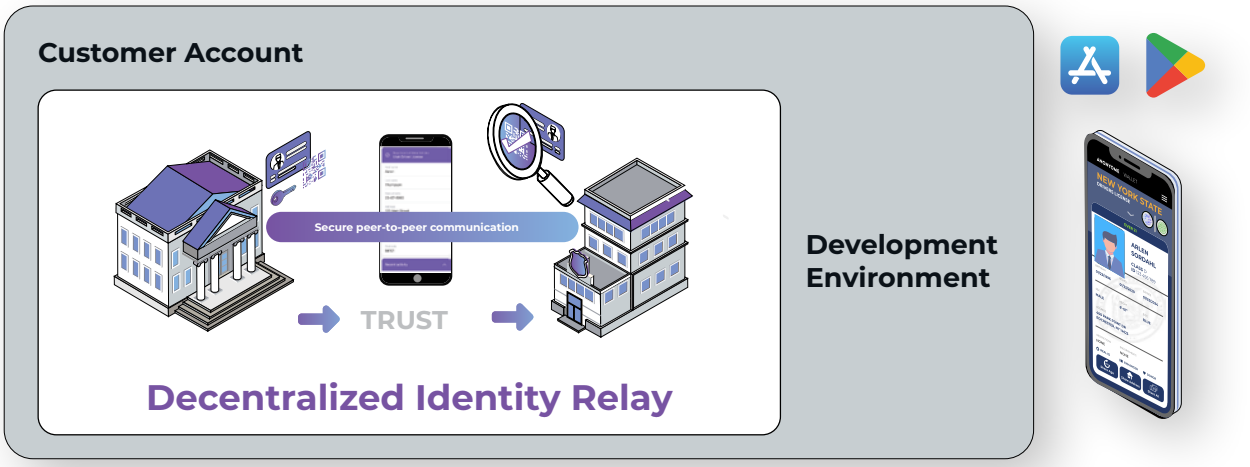



*Figure 1: Deploying the DI Wallet and Relay*

Note that there is an alternative to using the white label Decentralized Identity wallet. Anonyome Labs also provides a mobile wallet SDK that can be used to add the wallet functionality to a customer’s existing applications. For example, the customer may already have a mobile application deployed with its user base. Instead of the customer deploying a second application, the mobile wallet SDK allows the wallet functionality to be added to existing mobile applications.

Figure 2 (below) shows an example Decentralized Identity customer service deployment where the customer is using both a wallet and a Verifiable Credential Service. The verifiable credential service is used to issue and/or verify verifiable credentials. In the picture there is again one environment shown for the customer – development. As part of this environment is the Admin Console that provides a user-friendly interface for the Verifiable Credential Service.

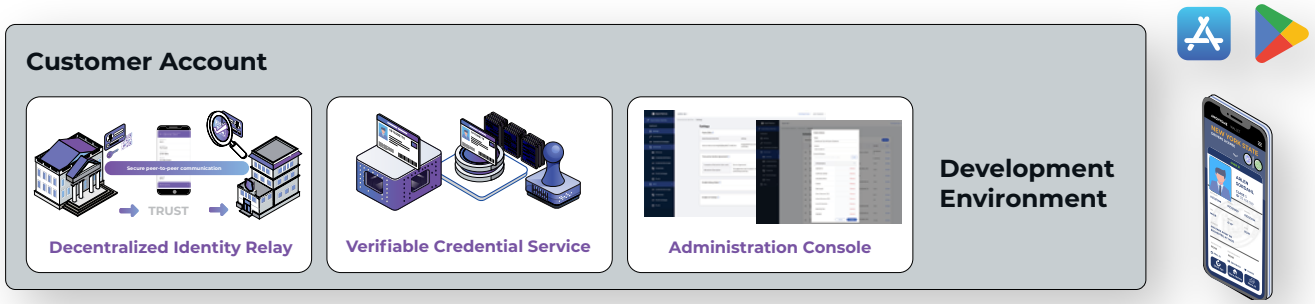



*Figure 2: A Customer Deployment of Anonyome Decentralized Identity Services*

Figure 3 (below) shows the Admin Console. The Admin Console allows the customer to exercise the full range of Verifiable Credential Service functions such as creating schema definitions and writing them to a ledger, creating DIDs and issuing credentials. It supports the issuing and verifying of both AnonCreds and W3C credentials.

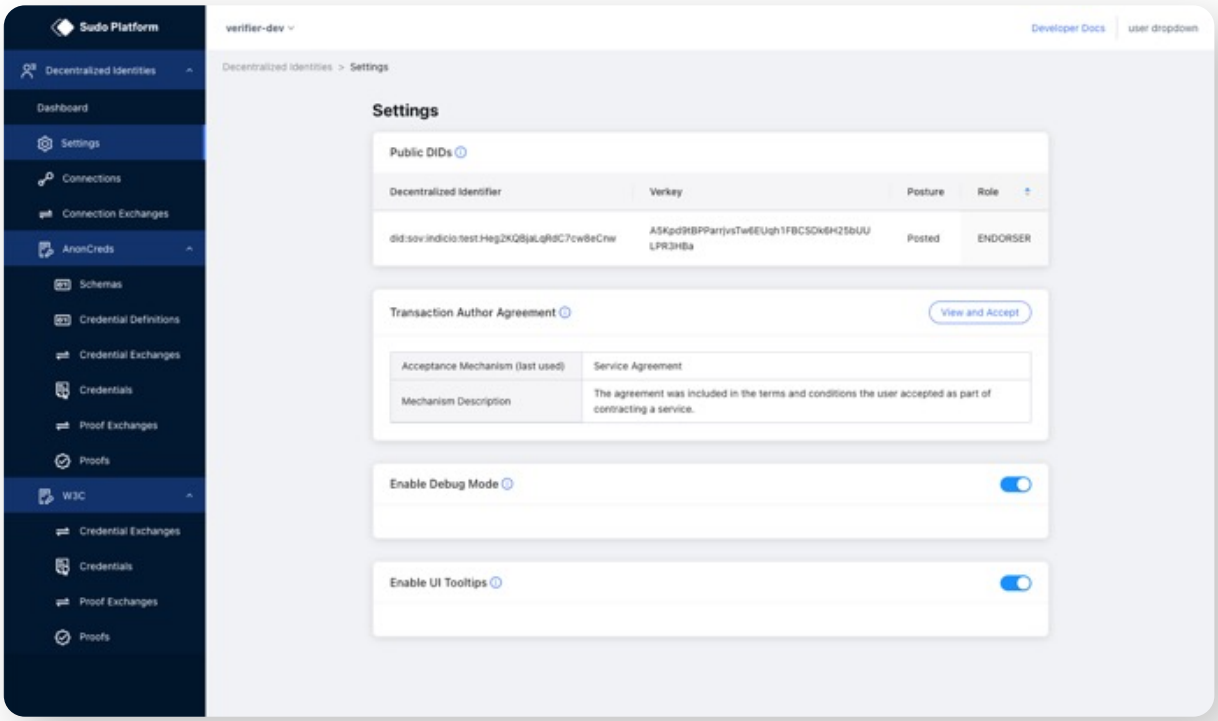



*Figure 3: Decentralized Identity Admin Console*

Figure 4 (below) shows the creation of a verifiable credential schema. In this case it's for and enterprise to report its Greenhouse Gas emissions

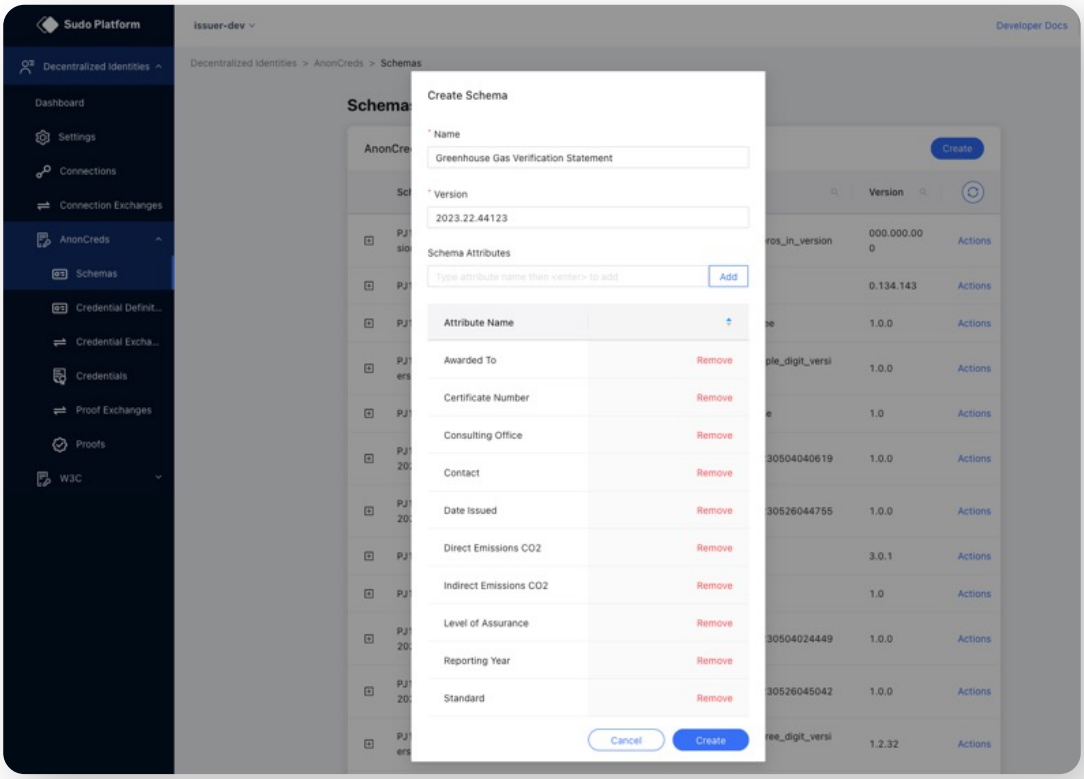



*Figure 4: Decentralized Identity Schema Development*

In many instances, customers require additional environments for testing and production. These new environments are created under the customer's account as well. They can also be deployed in a matter of hours. This is shown above in Figure 4. An additional test and production environments are depicted below.

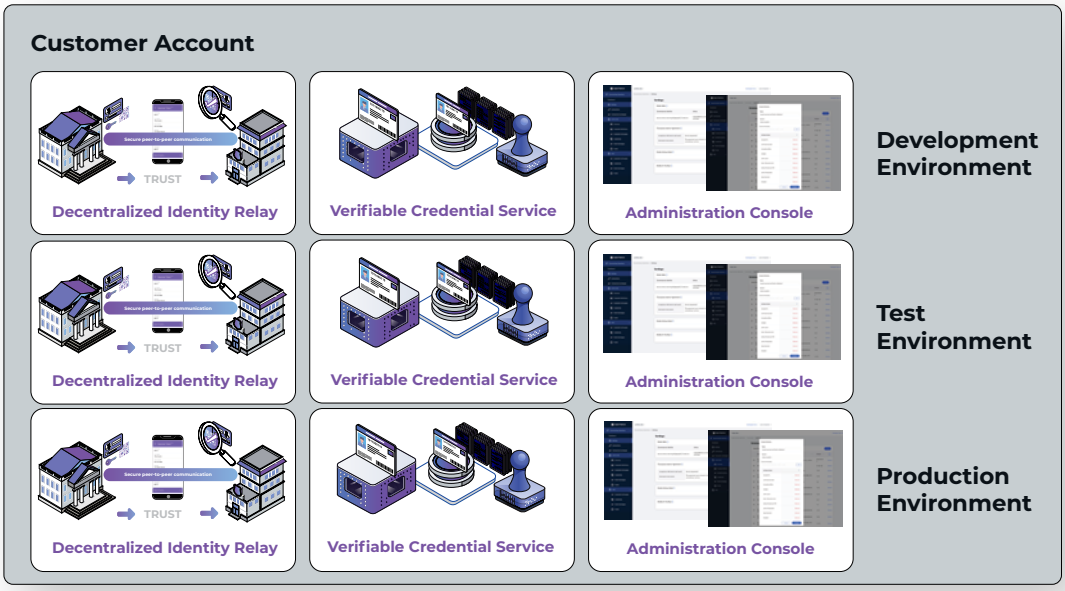



*Figure 5: A Customer Deployment with multiple environments*

# The Anonyome Platform Approach

## Automatic Service Updates

The Anonyome Platform services are being updated regularly. For example, the Verifiable Credentials Service is being enhanced to support additional credential protocols, credential types, and improvements to the Administration Console. Anonyome Labs provides testing and deployment of these updates to a customer's environment and no work is expected from the customer.

Anonyome Labs also performs any operating system or security patches as needed for the target environments.

## Protected by a Service Level Agreement

Anonyome Labs offers a service level agreement on all services that it provides to a customer to meet their uptime and other system requirements. This agreement details the timeliness of support response to various levels of priority issues. Anonyome provides 24x7 support by having support teams located both in the USA and Australia.

## High level of security and privacy

Anonyome Labs was founded by experts in identity, security, and privacy. When deploying the Sudo Platform services, Anonyome Labs' Deployment Specialists perform the installation according to exacting industry and company security standards.

Each deployment creates a Virtual Private Cloud with three subnets to isolate components based on function:

1. Public subnet - inbound, internet accessible, endpoints.
2. Private with NAT subnet - endpoints used by other internal components and which also require outbound access to the Internet
3. Private Isolated subnet - backend infrastructure components that do NOT require any internet access.

A Web Application Firewall (WAF) is also implemented to limit the types of http operations allowed in-bound and out-bound. It also provides protection from brute force attacks.

In addition, processes are in place for persistent storage backups and disaster recovery processes.

Alongside these items the customer also enjoys a completely separate account for their service components. It is not a multi-tenant model meaning there is no sharing of data storage or processing.

**Talk to us about Sudo Platform possibilities today.**

SUDO PLATFORM