# VeriSaaS Security Architecture

| Release | Date | Description | Author | Reviewer | Approver |
|---|---|---|---|---|---|
| 2.12 | 27/10/2020 | veriSaaS Security Architecture Q3 release | AMG | GSS | MSY |

# 1. Introduction

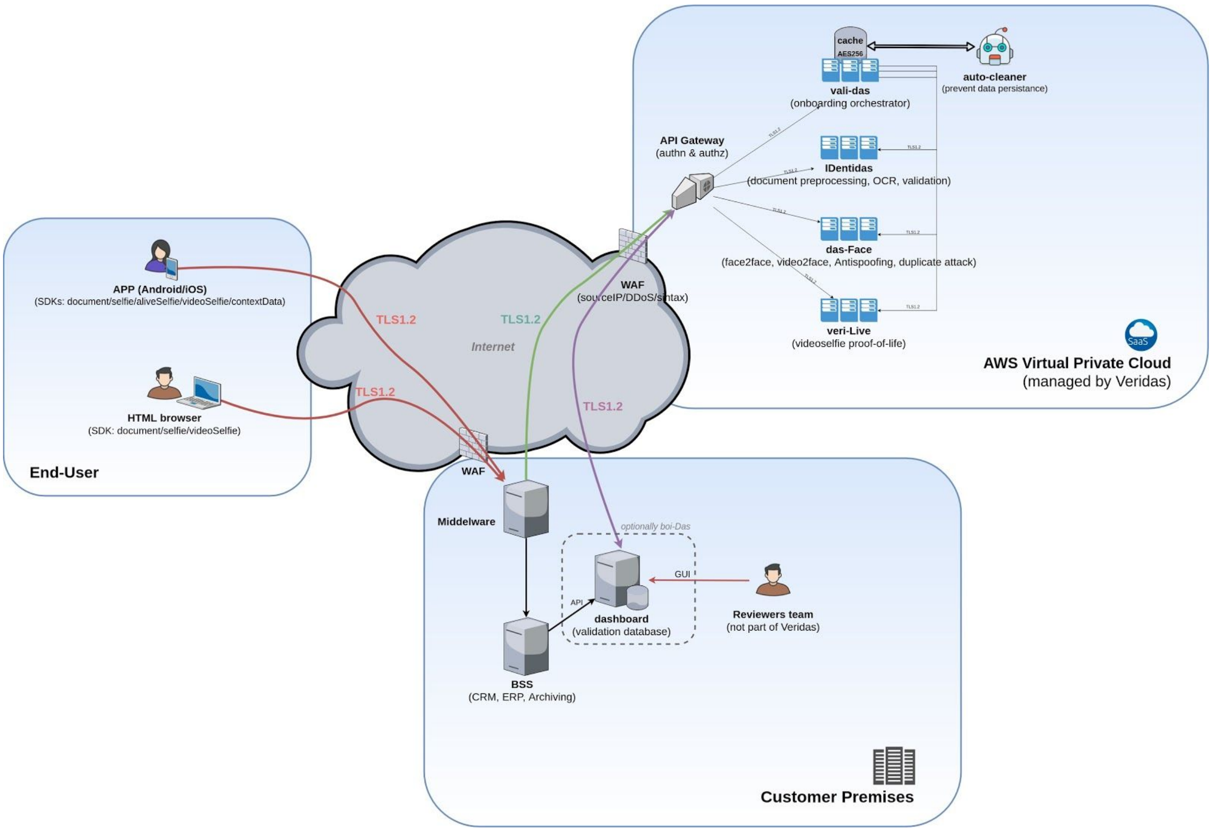
VeriSaaS Cloud is a cloud platform deployed in AWS infrastructure that provides a powerful execution environment for Veridas microservices. VeriSaaS cloud solves common deployment and operation issues allowing microservices to be independent from both infrastructure and the platform.

- Multitenancy: VeriSaaS Cloud is shared by different customers, and provides the mechanisms to logically isolate them.
- Security: VeriSaaS Cloud is built using the latest security standards for cloud deployed services. This document will explain the security architecture features in detail.
- Monitoring: VeriSaaS Cloud is monitored both from the outside (SLAs metrics) and the inside (CPU, RAM, disk and many others).
- Logging: VeriSaaS Cloud includes unified and centralized logging solutions. This is also important for the security of the environment as will be explained later on.
- Alerting: With the data insights provided by the security, monitoring and logging features VeriSaaS cloud sends alerts to Veridas Teams in order to quickly react  if any operational problem arises.
- Backup & Restore: VeriSaaS cloud has an Automated Backup and restore procedure for logs and configuration, so if a disaster happens, VeriSaaS Cloud is capable of resuming the service in a different region in less than 2 hours (RTO). No customer data is stored on the cloud, so RPO does not apply.

Current AWS regions in service are:

| **Service Area** | **Main Region** | **DR Region** |
|---|---|---|
| EMEA | Ireland (eu) | Frankfurt (eu4) |
| AMERS | North Virginia (us) | Oregon (us4) |

# 2. VeriSaaS Architecture



## 2.1. Architecture Overview

VeriSaaS Cloud exposes Services APIs in order to allow customers to consume Veridas OCR, document validation and biometric services without having to worry about on-premise deployments.

The Customer will be only responsible for Middleware, an on-premise application owned by them that is in charge of managing the communication between the End-User and VeriSaaS Cloud, and where most of the business logic resides.

The onboarding process basically is as follows:

1) An end-user starts the onboarding process capturing images of its document and biometric information typically using Veridas SDKs (HTML, IOS, Android). Veridas SDKs are not communicating, only performing an optimal capturing

2) The captured information will be sent to the customers' Middleware by the APP/web itself

3) The Middleware is in charge of conducting the customers business logic in addition to communicating with VeriSaaS Cloud Services. This communication must be performed using TLS1.2 protocol, and the Middleware has to be authenticated by VeriSaaS Cloud by the ApiKey header in every request. To Learn more about API-Key Authentication see section 5.5 below.

4) VeriSaaS processes all the images/videos uploaded by middleware.

5) The middleware or a backoffice platform may now retrieve from VeriSaaS the document OCR data, document and/or biometry scores, image cuts, etc.

6) Alternatively, Veridas offers an on-premises software solution (boi-das) for downloading, storing/archiving and reviewing all the validation processes

7) Finally, the validation is deleted by customer middleware/backoffice/boi-das. If that does not happen, Veridas auto-cleaner process will delete it after a pre-established expiration time (ie: 30mins)

# 3. Public Cloud provider

## 3.1. Why AWS?

### 3.1.1 Context

The first and one of the most important decisions is where to host the infrastructure needed to implement this SaaS platform. Given that the infrastructure will host multiple services and customers at the same time, we need certain warranties of scalability, availability, security, etc. Therefore, this is not a trivial decision and requires careful evaluation.

The chosen provider was AWS, for the following reasons:

- Technological leader: The Gartner consulting firm places AWS as the leader on both the completeness of vision and ability to execute categories, followed at a considerable distance by Microsoft Azure (the only other provider that makes it into the leader quadrant)

- Huge adoption (market share): AWS is the most used public cloud provider. It is estimated that AWS holds 40% of the total market share, which is more than the rest of the big players (Azure, Google Cloud, IBM) combined

- Reliability and Scalability: very large companies like Netflix host their entire infrastructure on AWS, which is a good sign of the abilities of AWS to scale an deliver reliable systems

- Feature rich: AWS is a mature platform with a huge catalog of products (and growing every day) that appeal to a wide range of use cases

- High availability: AWS offers data-center in various regions all around the world. In each region, multiple availability zones can be used to offer high-availability environments. Having multiple regions can help building global applications or deploy services that are compliant with data-residency regulations

- Security: AWS takes security very seriously and is compliant with major regulations like GDPR (Europe) or HIPAA (USA). Due to the sensitive nature of the data we are going to handle, this is a very important point.

- Extensive documentation, learning resources, support, and tooling: since AWS is the most used public cloud provider, there exists a lot of resources online that makes deploying any solution easier. AWS has a great community and a huge ecosystem of tools or integrations with other systems. It also provides a complete API to manage every resource on the cloud, so custom integrations can be developed easily.

We’ve also picked the AWS Ireland and North Virginia regions to deploy our services in, for the following reasons:

- First to receive updates: as it is considered the main region in Europe and the US, updates (both on hardware and products) will always arrive first to these regions by Amazon. AWS does gradual deployment of changes across regions (especially on hardware) and that means that some updates take weeks or months to be available on other regions after they’ve been released on Ireland

- Availability: the Ireland region consists of 3 availability zones (separate data-centers) and North Virginia consists of 6 AZs, which ensures high availability and resilience against natural disasters, electricity/network outages, etc.

## 4. Security Mechanisms

Here below some more details are provided on the security mechanisms currently implemented on our cloud-based solution.

## 4.1 TLS 1.2 protocol

All communications to VeriSaaS API must be done using HTTPS with the protocol TLS 1.2. Lower versions of the protocol are not allowed. Every communication inside VeriSaaS Cloud AWS VPC also uses TLS 1.2 providing an extra security layer to the HTTP traffic within the AWS VPC. TLS 1.2 is currently the latest security standard for secure HTTP communications.

## 4.2 SSL Certificates

When connecting to VeriSaaS Cloud, the HTTP traffic is encrypted by the server side using a valid certificate issued and maintained by AWS ACM. It is important that the customer should only trust a valid certificate (the CNAME of the certificate must be the correspondent to VerisaaS Cloud URL).

To learn more about AWS Certificates visit: https://aws.amazon.com/certificate-manager/

Note that certificate pinning is not a recommended practice, but in case you require it, please consider pining all of the AWS root CAs published at:

https://www.amazontrust.com/repository/

## 4.3 IP Source AllowList

As depicted in the architecture diagram in section 1, all requests to VeriSaaS Cloud must originate at a customer’s middleware. Veridas Customer Support requires at least one public IP address for the provisioning of a LIVE account, as this is a mandatory requirement for operating the service.

Once delivered the LIVE account for a Verisaas service, the Customer will be able to manage the AllowList associated to that service account by using Keymaker API service.

The AllowList can also be modified by reaching out to Veridas Service Desk (service SLA = 48-72h)

All requests coming from an unregistered source IP will be automatically discarded by VeriSaaS Cloud.

IP source AllowList is a mandatory requirement for all Veridas customers.

## 4.4 WAF

All incoming traffic to VeriSaaS Cloud gets first analized by a Web Access Filter. WAF is basically a firewall for web applications, filtering common attacks, such as SQL Injections or Path Traversal. In addition, WAF includes a DDoS protection (not only for layer 7 but also for 3 and 4 layers) to prevent attacks that could end up in a denial of service.

Veridas WAF also silently drops every incoming request that is not valid or having a malformed syntax or coming from a suspicious source network. By doing this, we protect our AWS VPC from undesired traffic that would only result in an increase of the resources load.

## 4.5 API Key authentication

In order to allow a Customer request to access a service, in addition to the fulfillment of the previous requirements, the incoming request must be authenticated by including an apikey header file with the correspondent Customer credential. A credential or API Key will be provided to the customer by Veridas Customer Support at the time of delivering the service. The customer’s middleware must add this header to all requests to Veridas API.

It is strongly recommended to rotate the apikey by the Customer prior to use it in a production environment. This can be achieved by using Keymaker API service.

Authentication is performed by the Veridas API Manager. Requests with the wrong API Key header will be rejected by the API manager.

Apikey example header: `‘apikey’: ‘wte5bk3273NP5xbbea8bG5Ca7795VyPWNz77’`

APIKEYs are passwords randomly generated by VeriSaaS, with a minimum length of 32 characters, and containing uppercase and lowercase letters, and numbers.

## 4.6 Request Throttling & Rate Limiting

In order to avoid problems caused by an accidental increase of traffic which may lead later into high costs to Customers, all customers' cloud accounts are set up with a maximum requests per minute limit. This maximum value is set to an upper limit high enough not to affect any normal operation. However, if for instance a process in the Customer’s middleware gets hung, it is possible that VeriSaaS Cloud could end up receiving an unusually high amount of traffic. To avoid these undesired situations, we implemented a request throttling mechanism that will monitor the amount of workload being received by each cloud service, and will artificially delay the excessed queries instead of dropping them.

Under these circumstances, Veridas operational team will inform the Customer so that proper action is taken. Nevertheless, It is also recommended that Customers anticipate Veridas Service Desk on any unusual traffic that may be reaching Veridas Cloud. This way, we proactively can take whatever measure is required to ensure the best service is provided.

If a Customer is willing to perform a stress or performance test against VeriSaaS Cloud is important to communicate to Veridas Customer Support beforehand, otherwise the test might be treated as an DDoS attack and will be repealed.

## 4.7 Continuous monitoring

Several monitoring tools are used on the VeriSaaS Cloud services and infrastructure, in order to detect any problem that can affect the service provided. Zabbyx, Cloudwatch and the ELK Stack Beats are some of the technologies used for this purpose.

An alerting system is also deployed, so the support team can be notified when any problem arises so they can react as quickly as possible.

## 4.8 Validations Auto-Cleaner

Veridas goal is avoid storing any Customer data in VeriSaaS Cloud for security reasons mainly.

Services like das-Face (face biometry engine) or das-Peak (voice biometry engine) are completely stateless, so each query is independent of the rest, and no data is stored in the cloud after the processing.

Validas on the other hand is a stateful service, as a validation process may require a number of queries to Veridas cloud (ie: upload obverse, upload reverse, upload selfie, etc…). As a consequence, Validas requires an operation database to temporarily cache the validation data before it is processed, and finally downloaded and deleted by the customer. If for some reason any validation is forgotten in the cloud without being deleted by the customer, Veridas takes care of it (deletes it) by means of an Autocleaner process.

Validations Auto-Cleaner deletes all validations that are due the established expiration time. This expiration time can be set up/customized for each customer. This time is usually lower than 30/60mins.

## 4.9 Encryption Data

VeriSaaS Cloud uses AWS KMS capabilities to encrypt data both in transit and at rest, for example in a shared Network File System, or in a database.

File system contents are encrypted using the Advanced Encryption Standard algorithm with XTS Mode and a 256-bit key (XTS-AES-256).

AWS KMS stores the master keys in highly durable storage in an encrypted format to help ensure that they can be retrieved when needed.

# 5. Legal & Compliance

Veridas has conducted a Data Protection Impact Assessment (DPIA), in accordance with General Data Protection Regulation (GDPR), in order to have a better knowledge of all the particularities of its processing.

Within the DPIA it was considered essential to analyse the infrastructure of the SaaS service itself as well as the provider (AWS). The Executive Summary of the DPIA is available to Veridas' Customers if required.

Regarding specific security measures, Veridas has also been certified on ISO/IEC 27001 on Apr 2020.