Technical and Organizational Measures
ALE Rainbow

Content

Preface

The objective of this document is to list the technical and organization measures in place at ALE, that concur to protect adequately not only data in general but also in particular personal data.

The objectives of such measures are based on meeting the standard control objectives of confidentiality, integrity and availability which represents a standard methodology to demonstrate that an adequate level of data protection exists and is efficient.

Identifying responsibilities:

In the context of the Rainbow Service, ALE is the editor and is the processor in all situations except when the Service is carried out from a private cloud operated by someone else than ALE. So, except in this latter situation, ALE is the data processor and is subcontracting the data center hosting & connectivity and the security thereof.

Certified safety

Rainbow is certified according to DIN ISO 27001:2013 ISO 27017 and ISO 27018, which can be viewed at any time at https://support.openrainbow.com/hc/fr/articles/360003802400-ISO-Certification-EN-

Hosting with OVH

OVH is committed to ensuring the optimal security of its infrastructures, including the implementation of an information systems security policy. Moreover, OVH infrastructures comply with numerous international standards and are certified according to PCI DSS, ISO/IEC 27001, SOC 1 TYPE II and SOC 2 TYPE II, etc.

Further information on data protection and data security at OVH can be found at https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml#accordion_1872-1.

1. Confidentiality

1.1 Physical Access Control and Security

Physical Access Protection; Data Center (OVH

The data center is operated by the provider OVH. Details of the security measures can be found at https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml.

General security measures of the physical locations
The physical access is based on a restrictive contextual security, which is effective from the entrance area. Each location is divided as follows:

- Private traffic areas
- Offices that are accessible to all employees and registered visitors
- Private offices accessible only to authorized personnel
- Areas with data center equipment
- Private data center areas
- Data center areas that house critical services
- General security measures of the physical locations

The following security measures are implemented to control access to OVH's physical locations:

- A policy for access authorizations
- Walls (or similar installations) between each area
- Cameras at the entrances and exits of the premises and in the server rooms
- Secured access, controlled by badge readers
- Laser barriers on the parking lots
- Motion detection system
- Burglar-resistant mechanisms at entrances and exits of data centers
- Mechanisms for detecting unauthorized intrusion (security service and video surveillance around the clock)
- Permanent monitoring center that monitors entrance and exit doors for opening

The physical access control is carried out by a badge system. Each badge is linked to an OVH account, which in turn is linked to a specific person. Thanks to this system, each person within the facilities can be identified and the control mechanisms authenticated:

- Any person entering OVH sites must have a personal badge linked to their identity.
- Each identity must be verified before a badge is issued.
- The badge must always be worn visibly within the premises.
- Badges must not show the name of their owner or the name of the company.
- It must be possible to immediately identify the category of persons present by means of the badge (employees, third parties, temporary access, visitors).
- The badge will be deactivated as soon as the holder is no longer authorized to access the premises.
- Badges of OVH employees are activated for the duration of the employment contract, for the other categories,
- The badge is automatically deactivated after a set period. Badges that are not used for three weeks are automatically deactivated.

Access at the doors by badges. This is the standard access control in the OVH premises:

- The door is connected to the central management system for access authorizations.
- The person must hold their badge to the special reader to unlock the door.
- Each access is checked during reading to ensure that the person has the appropriate authorization.
- In the event of a failure of the central management system for access authorizations, the authorizations configured at the time of the failure are valid for the entire duration of the incident.
- The door locks are protected against power failures and remain closed in these situations.

Access to the doors by key. Certain areas or equipment are locked with locks that can be locked with keys:

- The keys for each location are stored in a centralized area with restricted access and documented in an inventory list.
- Each key is provided with an identification label.
- An inventory of the keys is kept. Each use of the keys can be tracked by means of a provisioning mechanism or journal on paper.
- The inventory list of keys is checked daily against the inventory.

Access to the data centers through one-person locks. Access to our data centers is exclusively via single-person locks:

- Each airlock consists of two doors and a closed area between the controls to ensure that only one person passes at a time.
- One door can only be open when the other is closed (mantrap).
- The airlocks use the same badge system as the other doors and the same rules apply.
- Detection mechanisms check that only one person is in the lock (anti-piggybacking).
- The configuration of the system prevents the badge from being used more than once in the same direction (anti-passback).
- With a camera in the area of the airlock, accesses can be monitored.

Access to the goods locks. Goods are received into the data centers exclusively via the specially designed passageways:

- The delivery zone is configured in the same way as a single-person airlock, but with more space, no volume and weight checks and with badge readers only outside the airlock.
- Only the delivered article passes through the delivery zone, persons must enter through the one-person airlocks.
- In the delivery zone there is a camera without blind spot.

Access protection to ALE facilities

On ALE sites, there are teams having remote access to the Rainbow instance.

Physical Access Protection Measures

Locking systems
ALE usually uses electronic access control systems. The respective access authorizations are assigned organizationally and technically by authorized personnel. There are rules for handling electronic locking systems, for example how employees should behave if a transponder is lost.

Manual locking systems are sometimes still used for smaller ALE locations.

ID cards / ALE badges
ALE badges are mandatory and show the status (employee, visitor, guest, or non-employee). They remain the property of the company and must be visibly worn.

Visitor Policy
Visitors are registered and always accompanied by an ALE employee.

Sensitive areas
Access to sensitive areas (e.g. data center) is approved and recorded according to the minimum principle as required. Sensitive areas are also monitored outside of regular business hours.

Delivery and loading zones
Delivery and loading zones that are used for the reception or distribution of ALE assets are set up with an outer and inner door that are not opened at the same time.

Video surveillance
Video surveillance / closed circuit television (CCTV) covers the main entry points, main lobby, loading ramp and parking lots for large locations.

Clean Desk Policy
Every desk must be tidied up at the end of the working day, computers must be switched off.

Security windows
Window opening limiters are installed on the windows on the ground floor.

1.2 Access control to IT resources

Access control to infrastructure resources (hosting provider OVH)

- All employees use named user accounts.
- Connection sessions systematically have an expiration time adapted to each application.
- Before any change in authentication methods, the users' identity is verified.
- The use of standard, generic and anonymous accounts is prohibited.
- All access to resources is managed through individual SSH key authentication. Individual SSH key validity requires renewal every 3 days.
- All accesses are logged, stores and reviewed on a regular basis

Access control to infrastructure resources in ALE premises

Identity and Access Management

Identity and access management is based upon the job function or task to be achieved; and reflects the principles of separation of duties and least privilege.

Unique User ID and access
Each individual is assigned a unique **User ID** to access ALE information assets.

The account names shall allow discriminating between user, admin (privileged) and service accounts.

User ID / service account Authentication & Password management

Authentication mechanisms may be:
i) password / PIN or
ii) two-factor (such as password or PIN linked to a hardware device, software token or digital certificate).

Password Policy
Passwords have a minimum of eight (8) characters for user accounts and of twenty (20) characters for service accounts. Passwords have to contain three of for classes: upper case letters, lower case letters, digits, special characters.

Monitoring the use of ALE Information Systems

- Ensure compliance with applicable laws and regulations;
- Look for any violations of applicable laws and regulations;
- Ensure the effective use of Information Systems and their normal operation;
- Ensure the effective confidentiality and integrity of ALE data and compliance by Employees with their security obligations;

- Ensure the effective security of ALE Information Systems by implementing security threat detection features, including viruses, Trojans, worms, malware, and spam (unwanted messages), protection against these and judicial investigation.
- Ensure cost control.

(not limited to the above)

Organizational Measures

- Guidelines for authentication
- Guideline for information security
- Guideline for the use of intranet / internet
- Guideline for e-mail communication

Further technical measures

- Use of professional Firewalls
- Use of Anti-Virus Software
- Use of Intrusion Detection Systems
- Internet Proxy Management
- SSO/ SAML
- Restriction of access to servers

User access control in Rainbow

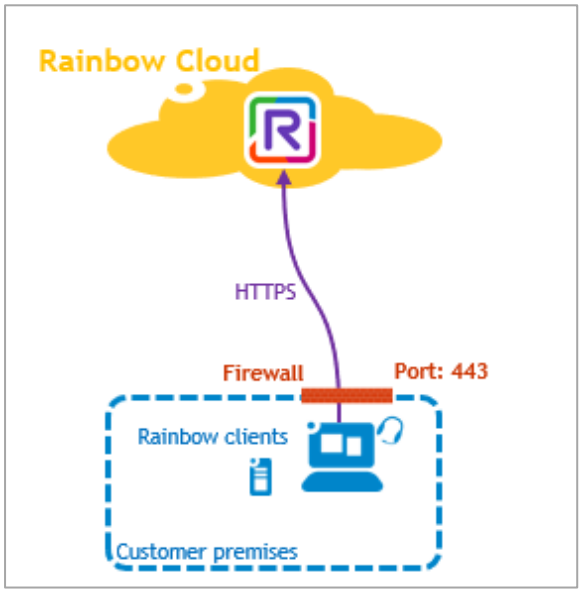
Rainbow offers different possibilities to authenticate users

a) Internal authentication

By default, Rainbow users are authenticated against the Rainbow service. In this case Rainbow knows how to verify user credentials and is responsible for the verification. When a user opens the Rainbow UCAAS application, the Rainbow login form is presented and used for authentication.

- Let Rainbow completely manage the login /password security rules.
- Under control of the Rainbow administrator.
- Nothing to configure, it is the default solution.

Internal Authentication



Internal authentication implements several security rules:

- During the self-registration, an email is sent to check the account creation.
- User passwords must respect a minimum complexity level
  At least 8 characters (64 maximum)
  - 1 lower-case letter
  - 1 upper-case letter
  - 1 number and
  - 1 special character.
- Password reset is secured by a temporary 6-digit PIN code sent to the user's email
- Then it must be entered at the password update phase

Access control to Rainbow services is based on role assigned by the administrator to users:
- Guest
- User
- Company Admin.

b) External authentication

Overview

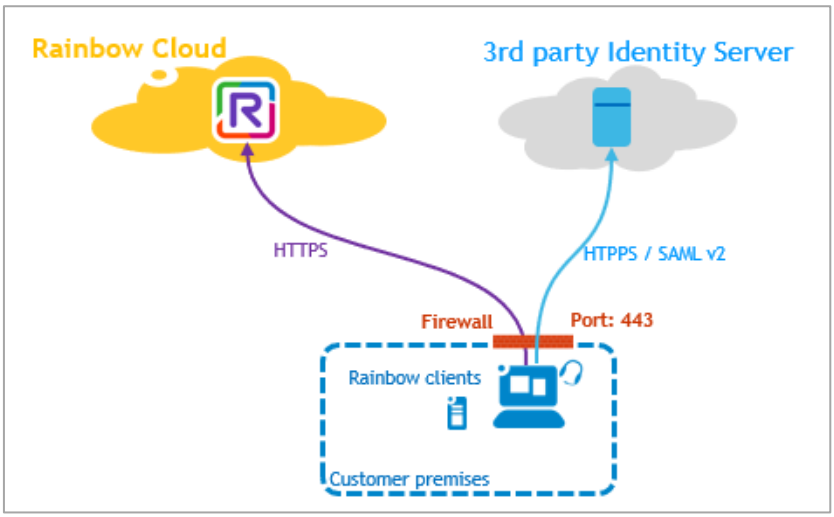
- Delegates the login / password security rules to an external centralized authentication server (e.g. MS Azure AD).
- Permit to share the same password with several applications
- Supports Cloud authentication servers only.
- Supported from PCs and smartphones (iOS, Android).
- Supports HTTPS/SAML v2 et OIDC (OpenID Connect) protocols.
- OIDC (OpenID Connect) is based on OAuth2
- SAML v2 (Security Assertion Markup Language)

Details

Rainbow solution is able to use an external identity provider based on SAML and OIDC. In this use case, for an administrative point of view, the administrator of the company authentication service needs to declare a new external service in the external identity service (as in the Microsoft Azure administrative interface) used by the company to let Rainbow interact with it when a user needs to log in.

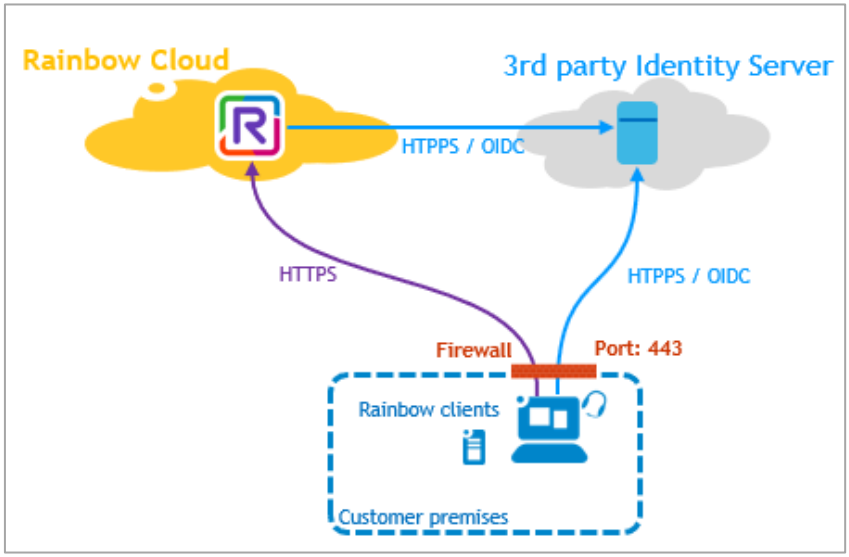
External authentication using SAML V2

Security Assertion Markup Language (SAMLv2) is a protocol used for authentication. This protocol is widely used as it is deployed in the enterprise world for a long time now. This technology is mainly based on Web browser interactions. This protocol is a way to give access to a protected resource, using a centralized authentication service without giving access to credential to external entities. For example, you can connect to your Rainbow account using your corporate login and password, but Rainbow must not have access to corporate credentials. As there is a decorrelation between the protected resource and the element that control the identity, SAMLv2 permits to the user to use the same credential to access to a wide range of protected resources or service. This use case is also well known under the Single Sign On (SSO) principle.



External authentication using OAuth2
OAuth2 is a framework designed to give authorization. It is more recent than SAMLv2, so it is less linked to Web browser and more API oriented. It became quickly very popular and widely used. OAuth2 is designed to give authorization and not authentication. A lot of application used OAuth2 to also perform authentication (and it is still the case). As to request authorization you need to identify the person, it is not an issue. But each application has to define a specific way to return the identity of the user to the external application. It is what OIDC is intended to do but under a well normalized format.

External authentication using OIDC
Open ID Connect (OIDC) is a protocol based on OAuth2 that permit to do authentication (as SAML does). OIDC is also used to perform SSO. OIDC inherits OAuth2 technologies and popularity and will replace SAMLv2 at the end.



Encryption and Security

- End-user passwords are hashed and salted in Rainbow's internal database.
- All data (IMs, files) exchanged between users or through bubbles are encrypted in transit and at rest.
- For transit, HTTPS + WSS through TLS 1.2/1.3 only
- At rest, AES 256-GCM is used
- Voice/Video communications are natively encrypted using WebRTC technology using DTLS & SRTP.
- All files uploaded by users are systemically scanned by an Antivirus (ClamAV) before storage and transmission.

1.3 Access control to data processing and data

Measures to manage access control to data processing and data at infrastructure hosting level (OVH)

- Access permissions are granted and tracked by supervisors according to the rule of least privilege and the principle of progressive trust.
- Wherever possible, all access permissions are based on roles and not on unit rights.
- Management of access rights and access permissions granted to a user or system is done through registration, modification and deregistration by supervisors, internal IT and Human Resources.
- Any remote access to OVH's information system is done via VPN. This requires a certificate known only to the user and a shared secret configured on the workstation.
- Data are encrypted at rest and in motion
- Cloud infrastructure provider does not have logical access to the servers.

Network security OVH

OVH manages a high-performance private fiber optic network connected to numerous operators and carriers. OVH manages its own backbone internally. It distributes connectivity to the local networks of each data center and interconnects them.

All equipment is secured by the following measures:

- Inventory management in a configuration management database
- Implementation of a hardening process, with instructions for the settings to be changed to ensure a secure configuration
- Access to the administrator functions of the devices is restricted via control lists
- All devices are managed by a bastion host using the principle of least privilege
- Backups are made of all configurations of network devices
- Logs are collected, centralized, and constantly monitored by the network operations team
- The implementation of configurations is automated and based on approved templates

Access Control of the OVH Cloud-IT-Systems

OVHcloud applies a strict policy to manage logical access rights. This policy contains the following provisions:

- Access rights are granted according to the "Least Privilege" principle.
- Access rights should be based on roles compared to specific rights of individual units.
- Granting of access to a user or system is managed based on initial access, modification, and removal provisioning procedures with the involvement of their managers, IT support / core services and HR.
- All employees use unique user ID accounts.
- Systematic timeout after a period of inactivity.
- The use of generic and / or anonymous user accounts is prohibited.
- A strict password policy is applied.
- Passwords should be generated randomly.
- Endpoint devices have a minimum password length of 10 alphanumeric characters.
- Saving passwords in unencrypted files, on paper or in web browsers is prohibited.
- Local password management software approved by IT Security is required.
- Remote access to OVH cloud IT systems must be via VPN. A password that is known to the user and a client certificate configured on the workstation must be used.

Measures to manage access to ALE IS/IT resources

Access policy
Accesses are controlled by the use of roles and authorizations, are logged and activities are monitored. Complete description exists in the ALE Security directive (ALE_000835).

Principles of access control

Business requirements of access control:
Authorizations granted under need to know principle Each User-ID may only access data, which is
a) non-confidential (open)
b) necessary for the fulfilment of individual professional tasks
c) granted by a superior

Access rights management:
N+1 managers are involved. IDs are blocked if unused.

System and application access control:

- Session control:
  There are many different IT resources to be accessed (network cession, desktop, mobile, router.) and each has specific rules for locking after invalid unsuccessful attempts.
- Advanced functions access:
  Those are subject to users consent (ex/ recording)
- Network Access Control:
  Whitelisting for wired access; encryption for wireless access.
- Access to External Network Services:
  All external network services are filtered by the company's security devices that only allow the protocols, ports, source & destination IP addresses, applications, and session timeouts. Service whitelisting in place.
- Outbound User Access:
  Use of proxy and traffic monitoring. Remote Access requires strong authentication.
- Remote Management & Diagnostic ports:
  Port management (disablement) helps manage such security.
- Network Segregation:
  Non-IT managed networks are segmented (even if there is no external connectivity). Routers or firewalls are used to only allow the required traffic, if any, to pass into the company network.
- Dual-homed Computers:
  Connecting to non-company network wit company assets is prohibited.
- Network Routing:
  ALE network routing and switching infrastructure are monitored for Denial of Service attacks. External access to network information pertaining to the internal company network is restricted
- Domain Name Service (DNS) is protected from non-trusted networks:
  Management of externally facing information, no internal DNS query forward.

Measures to manage access control to data processing and data at Rainbow

Role Definition

Rainbow users in an End Customer company may have one of the two following roles:

- Company Admin
  - Additionally to the rights of the simple User, he can administrate his company.

- As a simple User
  - Access to the Rainbow features will depend on his Rainbow subscription.

Restricting Access to File Sharing Feature
In order to control file exchanges between users, it is possible to restrict access to the “File Sharing” feature (upload and transfer). Configuration done by the company’s administrator for the whole company or user per user.

Restrict Change of Username
As a protection against usurpation, it is possible to forbid the modification by user of his title, first name and last name.

Encryption and Security

Encrypted Password Database Storage
End-user passwords are hashed and salted in Rainbow's internal database.

Encryption at transit and at rest

- All data (IMs, files) exchanged between users or through bubbles are encrypted in transit and at rest.
- For transit, HTTPS + WSS through TLS 1.2/1.3 only.
- At rest, AES 256-GCM is used.
- Voice/Video communications are natively encrypted using WebRTC technology using DTLS & SRTP.

Antivirus Scan for Files

All files uploaded by users are systemically scanned by an Antivirus (ClamAV) before storage and transmission.

1.4 Client segregation controls

Multi-client capability
- Rainbow is completely multi-client capable
- Logical separation of customer accounts

Client dedicated capabilities:
Rainbow Edge offer: https://support.openrainbow.com/hc/fr/articles/360012465520

Separation of test and production systems
- Test environment for new software applications or critical updates.
- Roll out only takes place after a successful test.

1.5 Pseudonymization

Pseudonymization of request Logs

All requests to the Rainbow application are logged

Logs are:

- completely anonymized.
- sent to a cluster of servers where they are stored redundantly.
- kept during the minimal duration imposed by law.

2. Integrity

2.1 Transfer controls

Encrypted communications in Rainbow

Any plain-text connections from internet are systematically denied

HTTPS connectivity is used only (443 port)

- WebSockets are then secured
- No other service is opened on public internet
- Access from 80 port is systematically redirected to 443 port

OpenSSL used for encryption is always maintained up to date.

SSLv2, SSLv3, TLS 1.0 and TLS 1.1 are disabled in favor of TLS 1.2 and TLS1.3

- Do not offer deprecated weak SSL support.
- Every HTTPS negotiation is done through TLS only

Standard Wildcard SSL/TLS certificates from Gandi / Comodo CA

- With a 256 bits ECDDSA key (elliptic curve) and signed with RSA-SHA256.
- No self-signed certificate used.

2.2 Input controls

Input Controls at ALE

Whether and by whom data has been entered, changed, or removed in IT systems can be subsequently checked and determined by:

- user profiles
- user identification
- Authorization concepts

Logging functions of all productive systems are working constantly and are held for a sufficient period of time.

Input control in Rainbow (Log Analysis)

Rainbow security abstract: https://support.openrainbow.com/hc/en-us/articles/115001019330

ALE Rainbow Operation team has the ability to precisely analyze the stored activity logs in case of:

- attack,
- suspect activity,
- or upon judicial requisition.

End customers and Business Partners do not have access to logs.

In case of necessity, ALE Operation team can extract punctually some information for them.

Logs analysis permits to find:

- The source IP address,
- The user's identity,
- The data and time of the requests,
- The type of the requests.

Die Protokollanalyse erlaubt niemals das Abrufen von:

- Konversationen / Gesprächen
- Passwörtern

3. Availability & Resilience

3.1 Availability control

Operational Continuity (Server)

The operational continuity of infrastructures (availability of devices, applications, and operating processes) is ensured by various measures:

- Continuous liquid and air cooling
- Continuous and redundant power supply
- Capacity management for the devices under the responsibility of cloud providers
- Technical support of the service
- Redundancy of devices and servers used for system administration
- In addition, other mechanisms, such as the backup of network device configurations, ensure that the system can be resumed in the event of a fault

Prevention of natural and environmental hazards

- Installation of lightning conductors to reduce the accompanying electromagnetic wave
- Establishment of cloud providers premises in areas not at risk of flooding or earthquakes
- An uninterruptible power supply (UPS) with sufficient capacity and auxiliary transformers with automatic load switching
- Automatic switchover to power generators with a minimum output of 24 hours
- Installation of a liquid cooling system for the servers (98% of the server rooms have no air conditioning)
- Use of heating ventilation and air conditioning (HVAC) units that keep temperature and humidity constant
- Management of a fire alarm system (fire drills are conducted in the data centers every 6 months)

Technical measures for availability

To ensure data high availability, different mechanisms are in place:

- Hardware level with HA disk
- Databases are clustered and replicated
- Users files and static data are stored 3 times on replicated Openstack Swift Object Storage servers

Backup of all databases

- Frequency: Hourly database file system snapshotting
- Daily database backup on 2 remote sites and providers

High Availability

- HA on servers, storage bays and disks under the responsibility of ALE
- Electric and network HA under the responsibility of the host (OVH).

Monitoring

A monitoring infrastructure is in place for all OVH services. This has several goals:

- Detection of production and safety incidents
- Monitoring critical functions and triggering alarms to the monitoring system
- Notification of the responsible persons and initiation of the corresponding procedures
- Guarantee of service continuity when performing automated tasks
- Verification of the integrity of the monitored resources

Business Continuity Plan (ALE)

ALE has established a business continuity plan based on ISO27001 and specified through the requirements of the ISO27018 (extension to ISO27001).

3.2 Resilience/ load capacity

DDOS protection and Firewall

Detailed information can be found here https://www.ovh.de/anti-ddos/.

Rainbow is protected against DDoS (Distributed Denial of Service) attacks thanks to the solution created by OVH called VAC (vacuum).

- Completely configured and managed by OVH.

VAC is a combination of technologies developed by OVH to:

- analyze data packets quickly in real-time
- divert your server's incoming traffic
- separate non-legitimate requests from others and let legitimate traffic pass through

It is seen as a black box in which filters are not disclosed for security reasons.

- It is hardware ASIC-based packet filtering equipment.

The VAC processes occur in four steps

1. pre-firewall
   It is fully managed by OVH, and applies rules that define filters directing data packets to the Firewall Network

2. Firewall Network
   The Firewall Network is a solution that limits exposure to attacks from the public network. It activates automatically as soon as a DDoS attack starts.

3. Shield
   The Shield intervenes if an attack uses an amplification technique (DNS amp, NTP amp). Armor is the most advanced filter in our VAC and mitigates the strongest attacks.

4. Armor
   Armor is the most advanced filter in the VAC and intervenes in mitigating the strongest attacks.

4. Procedures for regular review, assessment and evaluation (Art. 32 Abs. 1 lit. d GDPR; Art. 25 Abs. 1 GDPR)

A. Data protection - Management

The following policies, procedures or directives regarding data security are documented in the ISMS system of ALE:

- Obligation of all employees to maintain secrecy (data secrecy)
- Measures to raise awareness among employees.
- ALE Security Charter
- ALE Security Directives
- ALE Security Policy
- ALE Data Protection and Privacy Policy
- ALE GDPR policy
- Crisis Management Guidelines Policy & procedure
- Confidential Information Guideline Policy
- Information Management System
- Audits by the data protection officer
- Audits by external auditors
- Documented processing activities.
- Regular review of the technical and organizational measures.
- Careful selection of service providers (see also under Contract Management).
- Certification ISO27001 including ISO27017 and ISO27018

B. Data protection officer

Louis-Philippe Ollier

Mail: dataprivacy@al-enterprise.com

Phone: +331 5566 3147

The contact details of the DPO can also be found at https://www.al-enterprise.com/en/legal/privacy

C. Incident-Response-Management

OVH

An incident management process is in place. It enables the prevention, detection, and resolution of these events in the service management infrastructures and the service itself. This process includes:

- A guide to the classification of security events
- The handling of security events
- Simulation exercises for the crisis team
- Tests of the response plan for disturbances
- Customer communication within the framework of a crisis management team

These procedures are subject to a continuous improvement process for the monitoring and evaluation of faults, the entire fault management, and its corrective measures.

ALE

Crisis Management Guidelines Policy

Established and documented processes for handling incidents

- Defined responsibilities
- Defined reporting channels
- Data breach procedure

D. privacy by design

As a matter of principle, in the Rainbow Service, only data that is appropriate and necessary for business purposes is collected and processed. Procedures for automated data collection and processing are designed in such a way that only the necessary data is collected.

There is no behavior data management in Rainbow. No data collected for, generated in, or resulting from Rainbow activities or activities analysis are communicated nor sold to third parties.

Rainbow can be used with minimal information, an e-mail address, and a password.

E. Contract management

If subcontractors are used for data processing, certain requirements apply. These include ensuring the technical and organizational measures of the subcontractors in accordance with Art. 28 GDPR in conjunction with Art. 32 para. 1 GDPR.

The following requirements apply to a subcontracting relationship:

- Detailed information on the purpose, type and scope of the commissioned processing and use of personal data of the client in accordance with Art. 28 para. 3 GDPR. The corresponding details are contractually fixed.
- German / EU service providers have appointed a company data protection officer if an order is required by law and ensure through the data protection organization that he is appropriately and effectively integrated into the relevant operational processes.
- Verbal orders must be confirmed and documented in writing.
- Individual contracts are only awarded via named contacts.
- Only restrictive access authorizations are granted for the technical environments concerned. In case of external access to the system, access will be deactivated or blocked after the end of the cooperation.
- For the transmission of personal data to external service providers, a contract template for order data processing is available, which contains appropriate control regulations.
- ALE has established data protection agreements with all its interlocking parties where relevant, as per GDPR Art. 28 instructions.

Appendix – ALE Security Certification

ISO27001 : 2013

Certificat

Certificate

N° 2019/82126.2 **Page 1 / 2**

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL

exerçant sous la marque / *operating under the brand*

ALCATEL-LUCENT ENTERPRISE

pour les activités suivantes :
for the following activities:

DESIGN, IMPLEMENTATION AND SUPPORT OF CLOUD-BASED SOLUTIONS
TO INTEGRATE CUSTOMERS BUSINESS PROCESSES

Statement of Applicability "ISMS-ALE-StatementOfApplicability-PublicVersion" version 4

ont été évaluées et jugées conformes aux exigences requises par :
have been assessed and found to meet the requirements of:

ISO/IEC 27001 : 2013

et est déployé sur les sites suivants :
and is developed on the following locations:

32 AVENUE KLEBER FR-92700 COLOMBES

Liste des sites certifiés en annexe(s) / *List of certified locations on appendix(ces)*

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2019-03-26** Jusqu'au *Until* **2022-03-06**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probationary value.

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Seul le certificat électronique, consultable sur www.afnor.org, fait foi en temps réel de la certification de l'organisme. The electronic certificate only, available at www.afnor.org, attests in real time that the company is certified. Accréditation COFRAC n°4-0001, Certification de Systèmes de Management, Portée disponible sur www.cofrac.fr. COFRAC accreditation n°4-0001, Management Systems Certification, Scope available on www.cofrac.fr. AFAQ est une marque déposée. AFAQ is a registered trademark.

Flashez ce QR Code pour vérifier la validité du certificat

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 18 187 000 € - 479 076 002 RCS Bobigny - www.afnor.org

Certificat

Certificate

N° 2019/82126.2

Annexe / ***Appendix*** **n° 1**

ALE INTERNATIONAL

exerçant sous la marque / *operating under the brand*

ALCATEL-LUCENT ENTERPRISE

Liste complémentaire des sites entrant dans le périmètre de la certification :
Complementary list of locations within the certification scope:

ALE INTERNATIONAL 115-225 RUE SAINT EXUPERY FR-29806 BREST CEDEX 9

ALE INTERNATIONAL 1, ROUTE DU DOCTEUR SCHWEITZER FR-67408 ILLKIRCH CEDEX

ALE USA Inc 26801 WEST AGOURA ROAD PO BOX 636 US CALABASAS CA 91301

ISO27018 : 2014

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2020/86660.1

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL

pour les activités suivantes :
for the following activities:

DESIGN, IMPLEMENTATION AND SUPPORT OF CLOUD-BASED SOLUTIONS TO INTEGRATE CUSTOMERS BUSINESS PROCESSES.

Statement of Applicability "ISMS-ALE-StatementOfApplicability_v6_Public".

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of :

ISO 27018 : 2014

et est déployé sur les sites suivants :
and is developed on the following locations:

32 AVENUE KLEBER IMMEUBLE LES BOURGOGNES -92700 COLOMBES

26801 WEST AGOURA ROAD US-US CALABASAS CA 91301

1 ROUTE DU DR ALBERT SCHWEITZER -67408 ILLKIRCH CEDEX

115-225 RUE A DE ST EXUPERY ZAC PRAT PIP - GUIPAVAS FR-29806 BREST CEDEX 9

Ce certificat est valable à compter du (année/mois/jour)
This certificate is valid from (year/month/day) **2020-04-06** Jusqu'au *Until* **2023-04-05**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probatoiry value.

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Seul le certificat électronique, consultable sur www.afnor.org, fait foi en temps réel de la certification de l'organisme. *The electronic certificate only, available at www.afnor.org attests in real time that the company is certified.* AFAQ est une marque déposée. *AFAQ is a registered trademark.* CERTI F 0058.6 11/2018

Flashez ce QR Code pour vérifier la validité du certificat

ISO27017 : 2015

Certificat

Certificate

N° 2020/86659.1

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL

pour les activités suivantes :
for the following activities:

DESIGN, IMPLEMENTATION AND SUPPORT OF CLOUD-BASED SOLUTIONS TO INTEGRATE CUSTOMERS BUSINESS PROCESSES.

Statement of Applicability "ISMS-ALE-StatementOfApplicability_v6_Public".

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of :

ISO 27017 : 2015

et est déployé sur les sites suivants :
and is developed on the following locations:

32 AVENUE KLEBER IMMEUBLE LES BOURGOGNES -92700 COLOMBES

26801 WEST AGOURA ROAD US-US CALABASAS CA 91301

1 ROUTE DU DR ALBERT SCHWEITZER -67408 ILLKIRCH CEDEX

115-225 RUE A DE ST EXUPERY ZAC PRAT PIP - GUIPAVAS FR-29806 BREST CEDEX 9

Ce certificat est valable à compter du (année/mois/jour)
This certificate is valid from (year/month/day) **2020-04-06**

Jusqu'au
Until **2023-04-05**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probationary value.

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat