

# Technische und organisatorische Maßnahmen Für ALE Rainbow

## Inhalt

---

### **1. Vertraulichkeit**

Zutrittskontrolle  
Zugangskontrolle  
Zugriffskontrolle  
Trennungskontrolle  
Pseudonymisierung

### **2. Integrität**

Weitergabekontrolle  
Eingabekontrolle

### **3. Verfügbarkeit und Belastbarkeit**

Verfügbarkeitskontrolle

### **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Datenschutzmanagement  
Datenschutzbeauftragter  
Incident Response Management  
Datenschutzfreundliche Voreinstellungen  
Auftragskontrolle

## **Vorwort**

Ziel dieses Dokuments ist es, die bei ALE durchgeführten technischen und organisatorischen Maßnahmen aufzuzeigen, die dem Schutz von Daten, insbesondere personenbezogenen Daten, dienen.

Ziel dieser Maßnahmen ist die Sicherstellung der Kontrollziele Vertraulichkeit, Integrität und Verfügbarkeit, die eine Standardmethodik darstellen, um ein angemessenes Datenschutzniveau aufzuzeigen.

## **Beschreibung der Verantwortlichkeiten**

Im Rahmen des Rainbow Service ist ALE Datenverarbeiter und verantwortlich für die Datensicherheit, dies gilt auch beim Einsatz von Unterauftragnehmern. Dies trifft nicht zu, wenn der Dienst Rainbow auf dem Server eines Dritten (on premises) ausgeführt wird.

## **Zertifizierte Sicherheit**

Rainbow ist nach DIN ISO 27001:2013 ISO 27017 und ISO 27018 zertifiziert, die jederzeit zu <https://support.openrainbow.com/hc/fr/articles/360003802400-ISO-Certification-EN->

## **Hosting mit OVH**

***Da Rainbow bei OVH gehostet wird, gehen wir in diesem Dokument insbesondere auch auf die technischen und organisatorischen Maßnahmen bei OVH ein.***

OVH setzt sich für die optimale Sicherheit seiner Infrastrukturen ein, einschließlich der Umsetzung einer Sicherheitsrichtlinie für Informationssysteme. Darüber hinaus erfüllen OVH-Infrastrukturen zahlreiche internationale Standards und sind nach PCI DSS, ISO/IEC 27001, SOC 1 TYPE II und SOC 2 TYPE II usw. zertifiziert.

- Weitere Informationen zum Datenschutz und zur Datensicherheit bei OVH finden Sie unter <https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml>.
- Außerdem finden Sie eine Zusammenfassung hier <https://www.ovh.de/files/2018-06/plaquette-gdpr-DE-FINAL.pdf>.

# 1. Vertraulichkeit

## 1.1 Physische Zutrittskontrolle und -sicherheit

### Physische Zutrittskontrolle Rechenzentrum (OVH)

Das Rechenzentrum wird vom Anbieter OVH betrieben. Einzelheiten zu den Sicherheitsmaßnahmen finden Sie unter <https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml>.

#### Allgemeine Sicherheitsmaßnahmen der physischen Standorte

Der physische Zugriff basiert auf einer restriktiven Kontextsicherheit, die vom Eingangsbereich aus wirksam ist. Jeder Ort ist wie folgt unterteilt:

- Private Verkehrsbereiche
- Büros, die für alle Mitarbeiter und registrierten Besucher zugänglich sind
- Private Büros nur für autorisiertes Personal zugänglich
- Bereiche mit Rechenzentrumsausrüstung
- Private Rechenzentrumsbereiche
- Rechenzentrumsbereiche, in denen kritische Dienstleistungen untergebracht sind

#### Folgende Sicherheitsmaßnahmen werden umgesetzt, um den Zugang zu den physischen Standorten von OVH zu kontrollieren:

- Eine Policy für Zutrittsberechtigungen
- Wände (oder ähnliche Vorrichtungen) zwischen jedem Bereich
- Kameras an den Ein- und Ausgängen der Räumlichkeiten sowie in den Serverräumen
- Gesicherte Zugänge, kontrolliert durch Badge-Lesegeräte
- Laserbarrieren auf den Parkplätzen
- Bewegungsmeldesystem
- Einbruchhemmende Mechanismen an Ein- und Ausgängen der Rechenzentren
- Mechanismen zur Erkennung unerlaubten Eindringens (Wachdienst und Videoüberwachung rund um die Uhr)
- Ständiges Überwachungszentrum, das Ein- und Ausgangstüren auf Öffnen überwacht

#### Die physischen Zutrittskontrollen erfolgen durch ein Badge-System.

Jeder Badge ist mit einem OVH Account verknüpft, und dieser wiederum mit einer bestimmten Person. Dank dieser Maßnahme können jede Person innerhalb der Anlagen identifiziert und die Kontrollmechanismen authentifiziert werden:

- Jede Person, die Standorte von OVH betritt, muss einen mit ihrer Identität verknüpften persönlichen Badge besitzen.
- Jede Identität muss vor der Ausgabe eines Badge überprüft werden.
- Der Badge muss innerhalb der Räumlichkeiten stets sichtbar getragen werden.
- Badges dürfen weder den Namen ihrer Inhaber noch den Namen des Unternehmens zeigen.
- Es muss möglich sein, die Kategorie der anwesenden Personen anhand des Badge sofort zu identifizieren (Mitarbeiter, Dritter, temporärer Zutritt, Besucher).
- Der Badge wird deaktiviert, sobald der Inhaber nicht länger zum Zutritt zu den Räumlichkeiten berechtigt ist.
- Badges von OVH Mitarbeitern werden für die Dauer des Arbeitsvertrages aktiviert; für die anderen Kategorien wird der Badge nach einem festgelegten Zeitraum automatisch deaktiviert.
- Badges, die drei Wochen lang nicht verwendet werden, werden automatisch deaktiviert.

#### Zutritt an den Türen per Badges. Dies ist die Standard-Zutrittskontrolle in den Räumlichkeiten von OVH:

- Die Tür ist mit dem zentralen Managementsystem für Zutrittsberechtigungen verbunden.
- Die Person muss ihren Badge an das spezielle Lesegerät halten, um die Tür zu entsperren.

- Jeder Zutritt wird beim Auslesen überprüft, um sicherzustellen, dass die Person über die entsprechenden Berechtigungen verfügt.
- Bei einem Ausfall des zentralen Managementsystems für die Zutrittsberechtigungen gelten die zum Zeitpunkt der Störung konfigurierten Berechtigungen für die gesamte Dauer des Vorfalls.
- Die Türschlösser sind gegen Stromausfälle geschützt und bleiben in diesen Situationen geschlossen.

**Zugang zu den Türen per Schlüssel. Bestimmte Bereiche oder Geräte sind mit per Schlüssel verschließbaren Schlössern abgesperrt:**

- Die Schlüssel werden für jeden Standort in einem zentralisierten Bereich mit eingeschränktem Zutritt aufbewahrt und in einer Inventarliste dokumentiert.
- Jeder Schlüssel ist mit einem Etikett zur Identifikation versehen.
- Es wird ein Bestandsverzeichnis über die Schlüssel geführt.
- Jede Verwendung der Schlüssel kann mittels eines Bereitstellungsmechanismus oder Journals auf Papier zurückverfolgt werden.
- Die Inventarliste der Schlüssel wird täglich mit dem Bestandsverzeichnis abgeglichen.

**Zutritt zu den Rechenzentren durch Einpersonenschleusen. Der Zutritt zu unseren Rechenzentren erfolgt ausschließlich über Einpersonenschleusen:**

- Jede Schleuse besteht aus zwei Türen und einem abgeschlossenen Bereich zwischen den Kontrollen, um sicherzustellen, dass nur eine Person auf einmal passiert.
- Eine Tür kann nur offen sein, wenn die andere geschlossen ist (Mantrap).
- Die Schleusen verwenden dasselbe Badge-System wie die anderen Türen, und es gelten dieselben Regeln.
- Erkennungsmechanismen prüfen, dass sich nur eine Person in der Schleuse befindet (Anti-Piggybacking).
- Die Konfiguration des Systems verhindert, dass der Badge mehr als einmal in dieselbe Richtung verwendet werden kann (Anti-Passback).
- Mit einer Kamera im Bereich der Schleuse können die Zutritte überwacht werden.

**Zutritt zu den Warenschleusen. Der Wareneingang in die Rechenzentren erfolgt ausschließlich über die speziell dafür vorgesehenen Durchgänge:**

- Die Lieferzone ist genauso konfiguriert wie eine Einpersonenschleuse, jedoch mit mehr Platz, ohne Volumen- und Gewichtskontrollen sowie mit Badge-Lesegeräten nur außerhalb der Schleuse.
- Nur der gelieferte Artikel passiert die Lieferzone, Personen müssen über die Einpersonenschleusen eintreten.
- In der Lieferzone befindet sich eine Kamera ohne toten Winkel.

**Die Bewegungen von Besuchern und gelegentlichen Dienstleistern sind streng geregelt. Diese Personen werden bei ihrer Ankunft am Standort registriert und erhalten einen Besucher- oder Dienstleister-Badge:**

- Jeder Besuch muss zuvor angemeldet werden.
- Für Dritte ist immer ein Angestellter verantwortlich und sie werden immer begleitet.
- Jede Identität wird vor dem Zutritt zu den Standorten überprüft.
- Jeder Dritte besitzt einen persönlichen Badge für den Tag, den er vor Verlassen des Standorts zurückgeben muss.
- Alle Badges müssen sichtbar getragen werden.
- Die Badges werden am Ende des Besuchs automatisch deaktiviert.

## **Zutrittsschutz zu ALE-Räumlichkeiten**

*Bei ALE sitzen Teams mit der Berechtigung, per Remote auf Rainbow zuzugreifen. Daher werden an dieser Stelle die Zutrittsschutzmaßnahmen bei ALE aufgezeigt.*

### **Physischer Zutrittsschutz**

#### **Schließsysteme**

ALE verwendet in der Regel elektronische Zutrittskontrollsysteme. Manuelle Verriegelungssysteme werden manchmal noch für kleinere ALE-Standorte eingesetzt.

Die jeweiligen Zutrittsberechtigungen werden organisatorisch und technisch von autorisiertem Personal vergeben.

Jeder ALE Beschäftigte ist zur Einhaltung von Verhaltensregeln im Umgang mit elektronischen Schließsystemen verpflichtet. Insofern ein Transponder (oder Schlüssel) verloren geht, ist dies umgehend zu melden, um entsprechende Maßnahmen einzuleiten.

#### **Verpflichtung zum Tragen von Ausweisen / ALE Badges**

Das Tragen von ALE Badges ist verpflichtend und zeigt den Status des Trägers an (Mitarbeiter, Besucher, Gast oder Nicht-Mitarbeiter). Sie bleiben Eigentum des Unternehmens.

#### **Besucherreglung**

Besucher werden registriert und müssen zu jedem Zeitpunkt sichtbar einen Badge tragen und von einem ALE-Mitarbeiter begleitet werden.

#### **Sensible Bereiche**

Der Zutritt zu sensiblen Bereichen (z.B. Rechenzentrum) wird nach dem Minimalprinzip nach Erforderlichkeit genehmigt und registriert. Sensible Bereiche werden auch außerhalb der regulären Geschäftszeiten überwacht.

#### **Liefer- und Ladezonen**

Liefer- und Ladezonen, die für den Empfang oder die Verteilung von Lieferungen genutzt werden, sind mit einer Außen- und Innentür gesichert, die nicht gleichzeitig geöffnet werden können.

#### **Videoüberwachung**

Videoüberwachung (CCTV) deckt die wichtigsten Einstiegspunkte, Hauptlobby, Laderampe und Parkplätze für große Standorte ab.

#### **Clean Desk Policy**

Jeder Schreibtisch muss am Ende des Arbeitstages aufgeräumt werden, Computer müssen ausgeschaltet werden.

#### **Sicherheitsfenster**

Fensteröffnungsbegrenzer werden an den Fenstern im Erdgeschoss installiert.

## 1.2 Zugangskontrolle auf IT-Ressourcen

### Allgemeine Zugangskontrollmaßnahmen bei OVH

#### Personalisierte Nutzerkonten

- Alle Angestellten verwenden namentliche Benutzerkonten.
- Verbindungssitzungen haben systematisch eine für jede Anwendung angepasste Ablaufzeit.
- Vor jeder Änderung der Authentifizierungsmethoden wird die Identität der Benutzer überprüft.
- Die Nutzung von Standardkonten, generischen und anonymen Konten ist verboten.

#### Passwortpolitik

- Durch den Einsatz eines automatischen Passwortgenerators wählt der Benutzer sein Passwort nicht selbst.
- Die Mindestlänge eines Passwortes beträgt 10 alphanumerische Zeichen.
- Die Passwörter werden alle 3 Monate geändert.
- Benutzerkonten werden automatisch deaktiviert, wenn das Passwort nicht nach 90 Tagen geändert wird.
- Es ist verboten, Passwörter in unverschlüsselten Dateien, auf Papier oder in Webbrowsern zu speichern.
- Die Verwendung einer lokalen, vom Sicherheitsteam genehmigten Passwortverwaltungssoftware ist vorgeschrieben.
- Vergisst ein Benutzer sein Passwort, sind nur der Vorgesetzte des Mitarbeiters und der Sicherheitsbeauftragte berechtigt, es zurückzusetzen.

### Zugangs- und Zugriffssteuerung zu Infrastrukturressourcen bei OVH

#### Folgende Policy wird für die Verwaltung der Administratorzugriffe auf die Plattformen umgesetzt:

- Alle Administratorzugriffe auf ein System in Produktion erfolgen über einen Bastion Host.
- Administratoren verbinden sich via SSH mit den Bastion Hosts, indem sie individuelle und namentliche Paare öffentlicher und privater Schlüssel verwenden.
- Die Verbindung mit dem Zielsystem erfolgt entweder über ein Shared-Service-Konto oder über ein Namenskonto via Bastion Hosts
- Die Verwendung von Standardkonten auf den Systemen und Geräten ist verboten.
- Für Administrator-Fernzugriffe sowie für Zugriffe durch Mitarbeiter in sensiblen Umgebungen ist eine Zwei-Faktor-Authentifizierung mit vollständiger Nachverfolgung erforderlich.
- Administratoren verfügen zusätzlich zu ihrem Benutzerkonto über ein ausschließlich für administrative Aufgaben verwendetes Konto.
- Zugriffsberechtigungen werden von den Vorgesetzten gemäß der Regel der geringsten Berechtigung und dem Prinzip erworbenen Vertrauens erteilt und verfolgt.
- die SSH-Schlüssel sind durch ein Passwort geschützt, das die Anforderungen der Passwortpolicy erfüllt.
- Berechtigungen und Zugriffe werden regelmäßig in Zusammenarbeit mit den betreffenden Abteilungen überprüft.

#### Sicherung der Standardarbeitsplätze

Die folgenden Maßnahmen werden eingesetzt, um die Sicherheit der Standardarbeitsplätze des OVH Personals zu gewährleisten:

- Automatische Updateverwaltung
- Installation und Aktualisierung von Antivirus-Software mit regelmäßigen Scans • Ausschließliche Installation von Anwendungen aus einem genehmigten Anwendungskatalog
- Systematische Verschlüsselung der Festplatten
- Keine Administratorrechte für Mitarbeiter an ihrem Arbeitsplatz
- Festgelegte Vorgehensweise zur Behandlung potenziell kompromittierter Arbeitsplätze
- Standardisierung der Geräte
- Löschen der Sitzungen und Zurücksetzen der Arbeitsplätze beim Verlassen der Mitarbeiter

# Zugangskontrollmaßnahmen zu Infrastrukturressourcen in ALE-Standorten

## Identitäts- und Zugriffsverwaltung

Die Identitäts- und Zugriffsverwaltung basiert auf der zu erreichenden Aufgabenfunktion oder Aufgabe; und spiegelt die Grundsätze der Trennung von Pflichten und der geringsten Privilegien wider.

## Eindeutige Benutzer-ID und Zugriff

Jede Person erhält eine eindeutige **Benutzer-ID** für den Zugriff auf ALE-Informationsressourcen. Konto-IDs ermöglichen die Unterscheidung zwischen Benutzer-, Administrator- (privilegierten) und Dienstkonten.

## Benutzer-ID / Dienstkonto Authentifizierung & Kennwortverwaltung

Authentifizierungsmechanismen können

- Passwort / PIN oder
- Zwei-Faktor-Authentifizierung  
(z. B. Passwort mit Software-Token oder digitalen Zertifikat verbunden).

## Kennwortrichtlinien

Kennwörter haben

- mindestens acht (8) Zeichen für Benutzerkonten und
- zwanzig (20) Zeichen für Dienstkonten.

Kennwörter müssen drei von für Klassen enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen.

## Überwachung des Einsatzes von ALE-Informationssystemen

- Sicherstellung und Überwachung der Einhaltung der geltenden Gesetze und Vorschriften;
- Gewährleistung der effektiven Nutzung der Informationssysteme und ihres normalen Betriebs;
- Gewährleistung der effektiven Vertraulichkeit und Integrität der ALE-Daten und Einhaltung deren Sicherheitsverpflichtungen durch die Mitarbeiter;
- Sicherstellung der ALE-Informationssystem durch Funktionen zur Erkennung von Sicherheitsbedrohungen, einschließlich Viren, Trojaner, Würmer, Malware und Spam (unerwünschte Nachrichten).

## Organisationsmaßnahmen

- Richtlinien für die Authentifizierung
- Leitlinie für Informationssicherheit
- Leitlinie für die Nutzung von Intranet / Internet
- Leitlinie für die E-Mail-Kommunikation

## Weitere technische Maßnahmen

- Verwendung von Firewalls
- Verwendung von Anti-Virus-Software
- Internetproxyverwaltung
- SSO/ SAML
- Einschränkung des Zugriffs auf Server

## Benutzerzugangssteuerung in Rainbow

Rainbow bietet verschiedene Möglichkeiten, Benutzer zu authentifizieren

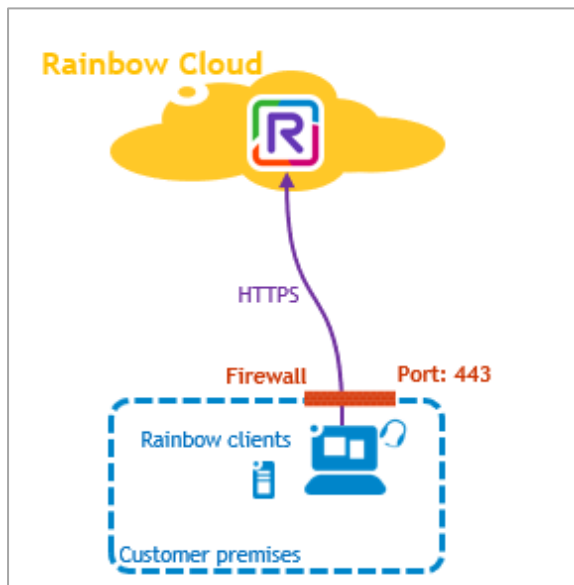
### a) Interne Authentifizierung (Standardlösung)

---

Standardmäßig werden Rainbow-Benutzer für den Rainbow-Dienst authentifiziert. In diesem Fall überprüft Rainbow die Benutzeranmeldeinformationen. Wenn ein Benutzer die Rainbow UCAAS-Anwendung öffnet, wird das Rainbow-Anmeldeformular angezeigt und für die Authentifizierung verwendet.

In der Standardlösung verwaltet Rainbow die Sicherheitsregeln für Login und Password unter der Kontrolle des Rainbow-Administrators.

#### Interne Authentifizierung



#### Die interne Authentifizierung implementiert mehrere Sicherheitsregeln:

- Während der Selbstregistrierung wird eine E-Mail gesendet, um die Kontoerstellung zu überprüfen.
- Benutzerkennwörter müssen eine Mindestkomplexitätsstufe einhalten  
Mindestens 8 Zeichen (maximal 64)
  - 1 Kleinbuchstaben
  - 1 Großbuchstaben
  - 1 Zahl und
  - 1 Sonderzeichen.
- Das Zurücksetzen des Kennworts wird durch einen temporären 6-stelligen PIN-Code gesichert, der an die E-Mail-Adresse des Benutzers gesendet wird. Dieser muss beim Aktualisieren des Kennworts eingegeben werden.

Die Zugriffssteuerung für Rainbow-Dienste basiert auf der Rolle, die der Administrator den Benutzern zugewiesen hat:

- Gast
- User
- Company Admin



## b) Externe Authentifizierung

---

### Übersicht

Die externe Authentifizierung delegiert die Anmelde-/Kennwortsicherheitsregeln an einen externen zentralen Authentifizierungsserver (z.B. MS Azure AD). Der Admin kann erlauben, dasselbe Kennwort für mehrere Anwendungen freizugeben.

- Unterstützt werden nur Cloud-Authentifizierungsserver.
- Nutzbar mit PCs und Smartphones (iOS, Android).
- Unterstützt HTTPS/SAML v2 und OIDC (OpenID Connect)-Protokolle.
- OIDC (OpenID Connect) basierend auf OAuth2
- SAML v2 (Security Assertion Markup Language)

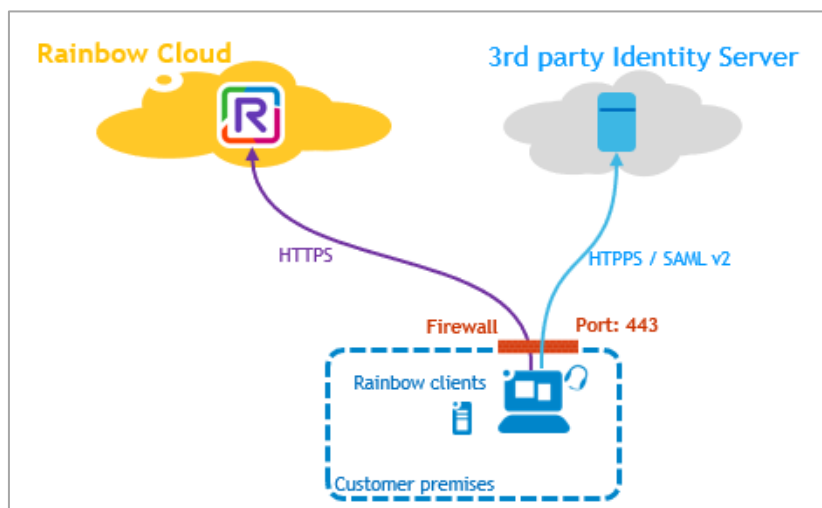
### Details

Rainbow ist in der Lage, einen externen Identitätsanbieter basierend auf SAML und OIDC zu verwenden. In diesem Anwendungsfall muss der Administrator des Authentifizierungsdienstes einen neuen externen Dienst im externen Identitätsdienst (wie in der Microsoft Azure-Verwaltungsschnittstelle) deklarieren. Rainbow interagiert mit diesem, wenn sich ein Benutzer anmeldet.

### Externe Authentifizierung mit SAML V2

Security Assertion Markup Language (SAMLv2) ist ein Protokoll, das für die Authentifizierung verwendet wird. Dieses Protokoll ist eine Möglichkeit, Zugriff auf eine geschützte Ressource zu gewähren, indem ein zentralisierter Authentifizierungsdienst eingesetzt wird.

Eine Verbindung zu Rainbow-Konten kann mit dem entsprechenden Firmen-Login und -Kennwort hergestellt werden. Da eine Dekorrelation zwischen der geschützten Ressource und dem Element besteht, das die Identität steuert, erlaubt SAMLv2 dem Benutzer, dieselben Anmeldeinformationen für den Zugriff auf eine Vielzahl geschützter Ressourcen oder Dienste zu verwenden. Dieser Anwendungsfall ist auch unter dem Single Sign On (SSO)-Prinzip bekannt.

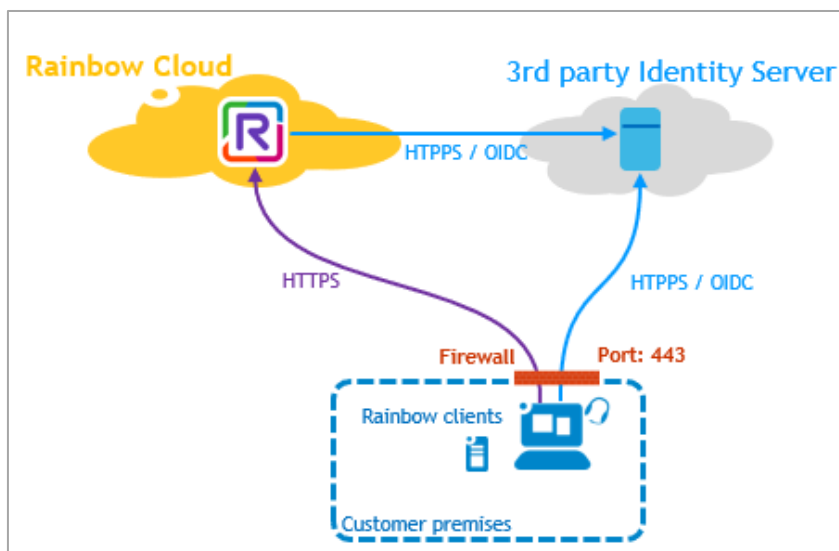


### Die externe Authentifizierung mit OAuth2

OAuth2 ist ein Framework, das die externe Autorisierung ermöglicht. Es ist neuer als SAMLv2 und ist primär API-orientiert.

### Die externe Authentifizierung mit OIDC

Open ID Connect (OIDC) ist ein auf OAuth2 basierendes Protokoll.



## Verschlüsselung und Sicherheit

- Endbenutzerkennwörter werden in der internen Datenbank von Rainbow gehasht.
- Alle Daten (IMs, Dateien), die zwischen Benutzern oder durch Bubbles ausgetauscht werden, werden während der Übertragung und im at rest verschlüsselt.
- Übertragung per HTTPS + WSS über TLS 1.2/1.3
- At rest kommt AES 256-GCM zum Einsatz.
- Die Sprach-/Videokommunikation wird mit DTLS & SRTP nativ verschlüsselt.
- Alle von Benutzern hochgeladenen Dateien werden vor der Speicherung und Übertragung von einem Antivirus (ClamAV) systemisch gescannt.

## 1.3 Zugriffskontrolle auf Datenverarbeitung und Daten

### Maßnahmen zur Verwaltung der Zugriffskontrolle auf Datenverarbeitung und Daten auf Infrastrukturhostingebene (OVH)

- Zugriffsberechtigungen werden von Supervisoren gemäß der Regel der geringsten Berechtigungen und dem Prinzip der progressiven Vertrauenswürdigkeit erteilt und nachverfolgt.
- Soweit möglich, basieren alle Zugriffsberechtigungen auf Rollen und nicht auf Einheitenrechten.
- Die Verwaltung der Zugriffsrechte und Zugriffsberechtigungen, die einem Benutzer oder System gewährt werden, erfolgt durch Registrierung, Änderung und Abmeldung durch Vorgesetzte, interne IT und Personalwesen.
- Jeder Fernzugriff auf das OVH-Informationssystem erfolgt über VPN. Dies erfordert ein Zertifikat, das nur dem Benutzer bekannt ist, und einen gemeinsam genutzten geheimen Schlüssel, der auf der Arbeitsstation konfiguriert ist.
- Die Daten werden at rest und während der Übertragung verschlüsselt.
- Der Cloudinfrastrukturanbieter hat keinen logischen Zugriff auf die Server.

## Netzwerksicherheit OVH

OVH verwaltet ein privates Hochleistungs-Glasfasernetz, das mit zahlreichen Betreibern und Spediteuren verbunden ist. OVH verwaltet seinen eigenen Backbone intern. Er verteilt die Konnektivität auf die lokalen Netzwerke jedes Rechenzentrums und verbindet diese untereinander.

Alle Geräte sind durch die folgenden Maßnahmen gesichert:

- Bestandsführung in einer Konfigurationsmanagementdatenbank
- Umsetzung eines Härtingsprozesses, mit Anleitungen für die zu verändernden Einstellungen, um eine sichere Konfiguration zu gewährleisten
- Zugriffe auf die Administratorfunktionen der Geräte sind über Kontrolllisten beschränkt
- Alle Geräte werden über einen Bastion Host unter Anwendung des Prinzips der geringsten Berechtigung verwaltet
- Von allen Konfigurationen der Netzwerkgeräte werden Backups erstellt
- Logs werden gesammelt, zentralisiert und ständig vom Netzbetriebsteam überwacht
- Die Implementierung von Konfigurationen erfolgt automatisiert und basiert auf genehmigten Vorlagen

## **Zugriffskontrolle der OVH Cloud-IT-Systeme**

OVH wendet eine strenge Richtlinie an, um logische Zugriffsrechte zu verwalten. Diese Richtlinie enthält die folgenden Bestimmungen:

- Die Zugriffsrechte werden nach dem "Least Privilege"-Prinzip gewährt.
- Die Zugriffsrechte sollten auf Rollen im Vergleich zu bestimmten Rechten einzelner Einheiten basieren.
- Die Gewährung des Zugriffs auf einen Benutzer oder ein System wird auf der Grundlage von Erstzugriffs-, Änderungs- und Entfernungsbereitstellungsverfahren unter Einbeziehung ihrer Manager, IT-Support /Kerndienste und HR verwaltet.
- Alle Mitarbeiter verwenden eindeutige Benutzer-ID-Konten.
- Systematische Auszeit nach einer Phase der Inaktivität;
- Die Verwendung generischer und/oder anonymer Benutzerkonten ist untersagt.
- Es wird eine strikte Kennwortrichtlinie angewendet.
- Kennwörter sollten nach dem Zufallsprinzip generiert werden.
- Endpunktgeräte haben eine minimale Kennwortlänge von 10 alphanumerischen Zeichen.
- Das Speichern von Passwörtern in unverschlüsselten Dateien, auf Papier oder in Webbrowsern ist verboten.
- Lokale Kennwortverwaltungssoftware, die von IT Security genehmigt wurde, ist erforderlich.
- Der Remote-Zugriff auf OVH-Cloud-IT-Systeme muss über VPN erfolgen. Es muss ein Kennwort verwendet werden, das dem Benutzer bekannt ist, und ein Clientzertifikat, das auf der Arbeitsstation konfiguriert ist.

## **Maßnahmen zur Verwaltung des Zugriffs auf ALE IS/IT-Ressourcen**

### **Zugriffsrichtlinien**

Zugriffe werden mithilfe von Rollen und Berechtigungen gesteuert, protokolliert und Aktivitäten überwacht. Dies ist umfassend in der ALE-Sicherheitsdirektive (ALE\_000835) dokumentiert.

### **Grundsätze der Zugriffskontrolle**

Berechtigungen werden nach dem Bedarfsprinzip erteilt. User dürfen nur auf Daten zugreifen, die

- a) nicht vertraulich (offen) sind
- b) für die Erfüllung individueller beruflicher Aufgaben erforderlich sind
- c) von einem Supervisor freigegeben wurden.

### **Verwaltung von Zugriffsrechten:**

N+1-Manager sind beteiligt. IDs werden blockiert, wenn sie nicht verwendet werden.

## **System- und Anwendungszugriffssteuerung:**

- Sitzungssteuerung:  
IT-Ressourcen, auf die zugegriffen werden kann (Netzwerkabteilung, Desktop, Mobil, Router...) haben spezifische Regeln für das Sperren nach ungültigen erfolglosen Zugriffsversuchen.
- Netzwerkzugriffssteuerung:  
Whitelisting für kabelgebundenen Zugriff; Verschlüsselung für den drahtlosen Zugriff.
- Zugriff auf externe Netzwerkdienste:  
Alle externen Netzwerkdienste werden von Security Devices des Unternehmens gefiltert. Nur bestimmte Protokolle, Ports, Quell- und Ziel-IP-Adressen, Anwendungen und Sitzungstimeouts sind zugelassen (Service Whitelisting).
- Ausgehender Benutzerzugriff:  
Verwendung von Proxy- und Datenverkehrsüberwachung. Der Remotezugriff erfordert eine starke Authentifizierung.
- Remoteverwaltungs- & Diagnoseports
- Netzwerksegregation:  
Nicht IT-verwaltete Netzwerke sind segmentiert (auch wenn keine externe Konnektivität vorhanden ist). Router oder Firewalls werden verwendet, um nur den erforderlichen Datenverkehr, falls vorhanden, in das Unternehmensnetzwerk passieren zu lassen.
- Dual-Homed-Computer:  
Das Herstellen einer Verbindung zu einem Netzwerk außerhalb des Unternehmens mit Unternehmensressourcen ist verboten.
- Netzwerkrouting:  
Die ALE-Netzwerkrouting- und Switching-Infrastruktur wird auf Denial-of-Service-Angriffe überwacht. Der externe Zugriff auf Netzwerkinformationen zum internen Unternehmensnetzwerk ist eingeschränkt.
- DNS (Domain Name Service) ist vor nicht vertrauenswürdigen Netzwerken geschützt.

## **Maßnahmen zur Verwaltung der Zugriffskontrolle in Rainbow**

### **Rollendefinition**

**Rainbow-Benutzer in einem Unternehmen haben grundsätzlich eine der folgenden Rollen:**

- Company Admin  
- Zusätzlich zu den Rechten des einfachen Benutzers kann er sein Unternehmen verwalten.
- Als einfacher User  
- Zugriff auf die Rainbow-Funktionen hängt sein Rainbow-Abonnement ab.

### **Einschränken des Zugriffs auf Dateifreigabefunktion**

Zur Steuerung des Dateiaustauschs zwischen Benutzern, kann der Zugriff auf die Funktion "Dateifreigabe" (Upload und Übertragung) eingeschränkt werden. Die Konfiguration kann durch den Administrator für das gesamte Unternehmen oder den einzelnen User eingestellt werden.

### **Sperrung von Änderungen der Benutzernamen**

Als Schutz vor Usurpation kann die Änderung von Titeln, Vornamen und Nachnamen durch den Benutzer verboten werden.

## Verschlüsselung und Sicherheit

### Verschlüsselte Kennwortdatenbankspeicher

Endbenutzerkennwörter werden in der internen Datenbank von Rainbow gehasht.

### Verschlüsselung bei Transit und at rest

- Alle Daten (IMs, Dateien), die zwischen Benutzern oder durch Blasen ausgetauscht werden, werden während der Übertragung und im Ruhezustand verschlüsselt.
- Für die Übertragung nur HTTPS + WSS über TLS 1.2/1.3.
- Im Ruhezustand wird AES 256-GCM verwendet.
- Die Sprach-/Videokommunikation wird mit DTLS & SRTP nativ verschlüsselt.

### Antivirus-Scan nach Dateien

Alle von Benutzern hochgeladenen Dateien werden vor der Speicherung und Übertragung von einem Antivirus (ClamAV) systemisch gescannt.

## 1.4 Steuerung der Clientsegregation

### Multi-Client-Fähigkeit

- Rainbow ist komplett multi-clientfähig
- Logische Trennung von Kundenkonten

### Client-dedizierte Funktionen:

Rainbow Edge Offer - Technical Overview - siehe <https://support.openrainbow.com/hc/fr/articles/360012465520>

### Trennung von Prüf- und Produktionssystemen

- Testumgebung für neue Softwareanwendungen oder wichtige Updates.
- Rollout findet erst nach einem erfolgreichen Test statt.

## 1.5 Pseudonymisierung

### Pseudonymisierung von Anforderungsprotokollen

Alle Anfragen an die Rainbow-Anwendung werden protokolliert.

Protokolle

- werden vollständig anonymisiert.
- werden an einen Servercluster gesendet, wo sie redundant gespeichert werden.
- werden während der gesetzlich vorgeschriebenen Mindestdauer aufbewahrt.

## 2. Integrität

### 2.1 Weitergabekontrolle

#### Verschlüsselte Kommunikation in Rainbow

Klartextverbindungen aus dem Internet werden systematisch verweigert

#### Es werden ausschließlich HTTPS-Verbindungen verwendet (Port 443)

- Web Sockets sind gesichert
- kein anderer Dienst wird im öffentlichen Internet geöffnet
- Der Zugang von Port 80 wird systematisch zu Port 443 umgeleitet

#### Aktualität

- OpenSSL wird immer auf dem neuesten Stand gehalten.

#### SSLv2, SSLv3, TLS 1.0 und TLS 1.1 sind zugunsten von TLS 1.2 und TLS1.3 deaktiviert

- Kein Einsatz veralteter SSL-Protokolle.
- Jede HTTPS-Aushandlung erfolgt nur über TLS

#### Standard Wildcard SSL/TLS Zertifikate von Gandi / Comodo CA

- mit einem 256-Bit-ECDSA-Schlüssel (elliptische Kurve) und mit RSA-SHA256 signiert.
- Es wird kein selbstsigniertes Zertifikat verwendet.

### 2.2 Eingabekontrolle

#### Eingabesteuerungen bei ALE

Ob und von wem Daten in IT-Systemen eingegeben, geändert oder entfernt wurden, kann nachträglich geprüft und bestimmt werden durch:

- Benutzerprofile
- Benutzeridentifikation
- Berechtigungskonzepte

Logging-Funktionen aller Produktivsysteme arbeiten ständig und werden ausreichend festgehalten.

## Eingabesteuerung in Rainbow (Protokollanalyse)

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

Das ALE Rainbow Operation Team hat die Möglichkeit, die gespeicherten Aktivitätsprotokolle genau zu analysieren, bei:

- Angriffen
- verdächtigen Aktivitäten,
- gerichtlicher Aufforderung.

Endkunden und Geschäftspartner haben keinen Zugriff auf Protokolle. Im Notfall kann das ALE Rainbow Operation Team punktuelle Informationen für sie extrahieren.

### Die Protokollanalyse ermöglicht die Suche nach:

- Die Quell-IP-Adresse,
- Die Identität des Benutzers,
- Die Daten und die Uhrzeit der Anfragen,
- Der Typ der Anforderungen.

### Die Protokollanalyse erlaubt keinen Zugriff auf:

- Gespräche / Konversationen
- Passwörter.

## 3. Verfügbarkeit & Resilienz

### 3.1 Verfügbarkeitskontrolle

#### Betriebskontinuität (Server)

Die Betriebskontinuität der Infrastrukturen (Verfügbarkeit von Geräten, Anwendungen und Betriebsabläufen) wird durch verschiedene Maßnahmen sichergestellt:

- Kontinuierliche Flüssigkeits- und Luftkühlung
- Kontinuierliche und redundante Stromversorgung
- Kapazitätsmanagement für die Geräte unter der Verantwortung von Cloud-Anbietern
- Technischer Support des Dienstes
- Redundanz von Geräten und Servern für die Systemadministration
- Darüber hinaus stellen andere Mechanismen, wie die Sicherung von Netzwerkgerätekfigurationen, sicher, dass das System im Falle eines Fehlers wieder aufgenommen werden kann.

## Vermeidung von Natur- und Umweltgefahren

- Installation von Blitzleitern zur Reduzierung der begleitenden elektromagnetischen Welle
- Gründung von Cloud-Anbietern in Gebieten, die nicht von Überschwemmungen oder Erdbeben bedroht sind
- Eine unterbrechungsfreie Stromversorgung (USV) mit ausreichender Kapazität und Hilfstransformatoren mit automatischer Lastumschaltung
- Automatische Umstellung auf Stromerzeuger mit einer Mindestleistung von 24 Stunden
- Installation eines Flüssigkeitskühlsystems für die Server (98% der Serverräume verfügen über keine Klimaanlage)
- Einsatz von Heizungs- und Klimaanlagen, -Einheiten, Temperatur und Luftfeuchtigkeit konstant halten
- Verwaltung einer Brandmeldeanlage (Brandübungen werden alle 6 Monate in den Rechenzentren durchgeführt)

## Technische Maßnahmen zur Verfügbarkeit

Um eine hohe Verfügbarkeit von Daten zu gewährleisten, gibt es verschiedene Mechanismen:

- Hardwareebene mit HA-Festplatte
- Datenbanken werden gruppiert und repliziert
- Benutzerdateien und statische Daten werden 3 Mal auf replizierten Swift Object Storage-Servern im offenen Stapel gespeichert

### Sicherung aller Datenbanken

- Häufigkeit: Stündliches Snapshot des Datenbankdateisystems
- Tägliche Datenbanksicherung an 2 Remote-Standorten

### Hohe Verfügbarkeit

- Hohe Verfügbarkeit auf Servern, Storage Bays und Festplatten unter der Verantwortung von ALE
- Electric und Network Verfügbarkeit unter der Verantwortung des Hosts (OVH).

## Überwachung

Für alle OVH-Dienste ist eine Überwachungsinfrastruktur vorhanden. Dies hat mehrere Ziele:

- Erkennung von Produktions- und Sicherheitsvorfällen
- Überwachung kritischer Funktionen und Auslösen von Alarmen im Überwachungssystem
- Mitteilung der verantwortlichen Personen und Einleitung der entsprechenden Verfahren
- Garantie der Servicekontinuität bei der Ausführung automatisierter Aufgaben
- Überprüfung der Integrität der überwachten Ressourcen

## Business Continuity Plan (ALE)

ALE hat einen Business Continuity Plan auf Basis von ISO27001 erstellt und durch die Anforderungen der ISO27018 (Erweiterung auf ISO27001) festgelegt.



## 3.2 Belastbarkeit/Belastbarkeit

### DDoS-Schutz und Firewall

Detaillierte Informationen finden Sie hier <https://www.ovh.de/anti-ddos/>.

Rainbow ist dank der von OVH erstellten Lösung VAC (Vacuum) vor DDoS-Angriffen (Distributed Denial of Service) geschützt. Diese wird vollständig von OVH verwaltet.

VAC ist eine Kombination von Technologien, die von OVH entwickelt wurden, um:

- Datenpakete schnell in Echtzeit analysieren
- den eingehenden Datenverkehr Ihres Servers umzuleiten
- nicht-legitime Anfragen von anderen zu trennen und legitimen Datenverkehr passieren zu lassen

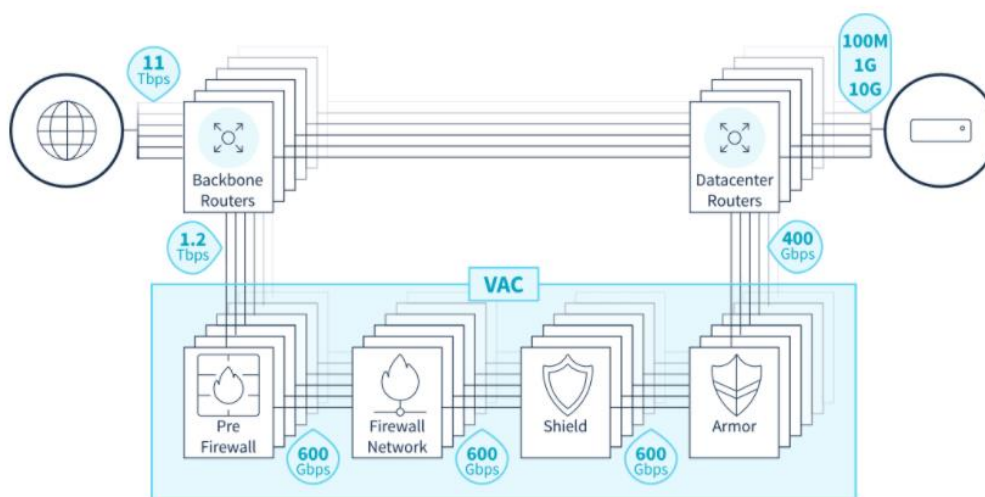
Es wird als Blackbox betrachtet, in der Filter aus Sicherheitsgründen nicht offengelegt werden.

- Es handelt sich um Hardware-ASIC-basierte Paketfiltergeräte.

#### Die VAC-Prozesse erfolgen in vier Schritten

1. Pre-Firewall  
Die vorgelagerte Firewall ist das erste Element unseres VAC Systems. Sie wird vollständig von OVH verwaltet und wendet Regeln an, nach denen Filter Datenpakete zum Firewall Network weiterleitet.
2. Firewall Network  
Firewall Network ist das zweite Element des VAC. Es ist eine Lösung, mit der das Risiko von Angriffen aus dem öffentlichen Netzwerk reduziert wird. Firewall Network wird automatisch bei jedem DDoS-Angriff aktiviert.
3. Shield  
Shield greift im Fall von Amplification-Angriffen (DNS Amp, NTP Amp, ...) ein.
4. Armor  
Armor ist der fortschrittlichste Filter unseres VAC und ist für die Abwehr der ausgefeiltesten DDoS-Angriffe zuständig.

Shield und Armor werden bei gezielteren Angriffen aktiv und ermöglichen es, den Prozessor des Servers zu entlasten, indem sie einen Teil der Filterung übernehmen.



## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Bewertung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### A. Datenschutz - Management

Die folgenden Richtlinien, Verfahren oder Richtlinien zur Datensicherheit sind im ISMS-System von ALE dokumentiert:

- Geheimhaltungspflicht aller Mitarbeiter (Datengeheimnis)
- Maßnahmen zur Sensibilisierung der Mitarbeiter.
- 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 durch den Datenschutzbeauftragten
- Audits durch externe Prüfer
- Dokumentierte Verarbeitungsaktivitäten.
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen.
- Sorgfältige Auswahl der Dienstleister (siehe auch unter Vertragsmanagement).
- Zertifizierung ISO27001 einschließlich ISO27017 und ISO27018

### B. Datenschutzbeauftragter

Louis-Philippe Ollier

Mail: [dataprivacy@al-enterprise.com](mailto:dataprivacy@al-enterprise.com)

Telefon: +331 5566 3147

Die Kontaktdaten des DSB finden Sie auch: unter <https://www.al-enterprise.com/en/legal/privacy>

### C. Incident-Response-Management

#### OVH

Ein Vorfalldmanagementprozess ist vorhanden. Es ermöglicht die Prävention, Erkennung und Lösung dieser Ereignisse in den Service-Management-Infrastrukturen und dem Dienst selbst. Dieser Prozess umfasst:

- Leitfaden zur Klassifizierung von Sicherheitsereignissen
- Der Umgang mit Sicherheitsereignissen
- Simulationsübungen für das Krisenteam
- Tests des Reaktionsplans auf Störungen
- Kundenkommunikation im Rahmen eines Krisenmanagement-Teams

Diese Verfahren unterliegen einem kontinuierlichen Verbesserungsprozess zur Überwachung und Bewertung von Fehlern, dem gesamten Fehlermanagement und seinen Korrekturmaßnahmen.

#### ALE

Richtlinien für das Krisenmanagement

Etablierte und dokumentierte Prozesse für den Umgang mit Vorfällen

- Definierte Verantwortlichkeiten
- Definierte Berichtskanäle
- Verfahren zur Verletzung von Daten

## D. Datenschutzfreundliche Voreinstellungen

Grundsätzlich werden im Rainbow Service nur Daten gesammelt und verarbeitet, die für geschäftliche Zwecke geeignet und notwendig sind. Verfahren zur automatisierten Datenerfassung und -verarbeitung sind so konzipiert, dass nur die notwendigen Daten erfasst werden.

Es gibt keine Verhaltensdatenverwaltung in Rainbow. Es werden keine Daten, die für die Rainbow Aktivitäten oder Aktivitätenanalyse gesammelt wurden oder die sich aus der Analyse von Rainbow ergeben, an Dritte weitergegeben oder verkauft.

Rainbow kann mit minimalen Informationen, einer E-Mail-Adresse und einem Passwort verwendet werden.

## E. Vertragsmanagement

Wenn bei der Datenverarbeitung Unterauftragnehmer eingesetzt werden, gelten bestimmte Vorgaben. Hierzu zählt die Sicherstellung der technischen und organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO i.V.m. Art. 32 Abs. 1 DSGVO.

Folgende Voraussetzungen für ein Unterauftragsverhältnis gelten:

- Es bestehen detaillierte Angaben über Zweck, Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers nach Vorgabe des Art. 28 Abs. 3 DSGVO. Die entsprechenden Angaben sind vertraglich fixiert.
- Deutsche / EU Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt, sofern eine Bestellung gesetzlich vorgeschrieben ist und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Mündliche Aufträge müssen schriftlich bestätigt und dokumentiert werden.
- Eine Vergabe von Einzelaufträgen erfolgt nur über namentlich benannte Ansprechpartner.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

# 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 probatory value.

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



Flashez ce QR Code  
pour vérifier la validité  
du certificat

Seul le certificat électronique consultable sur [www.afnor.org](http://www.afnor.org), fait foi en l'absence d'original de la certification de l'organisme. The electronic certificate only, available at [www.afnor.org](http://www.afnor.org),  
 stands as real title that the company is certified. Association COFRAC n°6 000. Certification de Systèmes de Management. Pointe de dépôt sur [www.afnor.org](http://www.afnor.org).  
 COFRAC accréditation n°19 0001. Management System Certification. Marque déposée sur [www.afnor.org](http://www.afnor.org).  
 AFNOR est une marque déposée. AFNOR is a registered trademark. CERTIF 19 0001.19 0001.



# Certificat

Certificate

N° 2019/82126.2

Page 2 / 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**



# Certificat

Certificate

N° 2020/86660.1

Page 1 / 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 probatory value.

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



Seul le certificat électronique, consultable sur [www.afnor.org](https://www.afnor.org), fait foi en temps réel de la certification de l'organisme. The electronic certificate only, available at [www.afnor.org](https://www.afnor.org), attests in real time that the company is certified. AFNOR est une marque déposée. AFNOR is a registered trademark. CERTIF: F 2008.0 1102076

Flashez ce QR Code pour vérifier la validité du certificat



# Certificat

Certificate

N° 2020/86659.1

Page 1 / 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 probatory value.

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



Ceci est un certificat électronique. Consultez le site [www.afnor.org](http://www.afnor.org) pour les en savoir plus de la certification de l'organisme. The electronic certificate only. Available at [www.afnor.org](http://www.afnor.org)  
Questo è un certificato elettronico. Consultare il sito [www.afnor.org](http://www.afnor.org) per saperne di più sulla certificazione dell'organismo. P. 0262.3 - 1/2021

Flâchez ce QR Code pour vérifier la validité du certificat