ALE | Where Everything Connects

Rainbow™

Rainbow Security Overview

Technical Business Engine

January 2021

Patrick LEMONNIER

Alcatel·Lucent Enterprise

History

Edition 01:	First edition of the document “Rainbow Security” (December 2019)
Edition 01a:	Adjustments on password protection and companies visibility
Edition 01b:	Adding information on password encryption and backup retention
Edition 01d:	Adding a section for data deletion
Edition 01e:	Adding a section for SMTP server

Disclaimer

This documentation is provided for reference purposes only and does not fully describe the capabilities of each Product and related features. Therefore, ALE International declines any liability for inaccuracies contained herein. For an exhaustive view on features list and product limits for the current product release please see the required Feature List/Product Limits document available through the ALE eBusiness Portal web site.

In the interest of continued product development, ALE International reserves the right to make improvements or other changes to this document and the products it describes at any time without prior notice.

Copyright

Agenda

1. Introduction
2. Overview
3. Hosting partner level
4. Architecture level security
5. User level security
6. Data level security
7. Transport layer security
8. Security auditing
9. Certification and compliance
10. Conclusion

Introduction

Introduction

❑ The objective of this presentation is to provide an overview of the different security elements put in place in the Rainbow ecosystem.

❑ This document is not necessarily technically exhaustive but provides a first level of knowledge on Rainbow security aspects to exchange with partners and customers.

❑ This document suits completely to people with Sales, Pre-Sales and solution designer roles.

❑ Here and there in this presentation, there are references to on-line information which provide additional information.

Overview

❑ The implementation of security on Rainbow has been done early in the design of the Rainbow solution.

❑ The security rules cover all levels of the Rainbow architecture, including both the hardware part and the software part.

❑ This concerns:

- The availability of servers and data.
- The securing of transport and storage of data.
- The functions of Authentication, Authorization and Accounting.
- The administration of companies in a multi-company environment.

❑ In addition, to ensure continuity and reliability of security rules, security audits are performed regularly.

❑ Finally, local regulations in different countries have been taken into account to some extent.

HOSTING PARTNER LEVEL

OVH Premises security

Hosting partner premises (1/2)

❑ Physical security

▪ Physical Access Control:

- All access to the OVH premises is strictly monitored.
- Every member of staff receives a RFID name badge which is also used to restrict their access.
- To prevent any intrusions or hazards, every boundary is secured using barbed-wire fencing and 24/7 video surveillance.

▪ Security against Fire:

- Every data center room is fitted with a fire detection and extinction system, as well as fire doors.
- OVH complies with the APSAD R4 rule and has N4 conformity certification.

▪ Electrical Supply:

- Datacenters are powered by two separate electrical power supplies and are also equipped with UPS devices.
- Power generators have an initial autonomy of 48hrs to counteract any failure of the electricity supply network.

▪ Network Connectivity:

- OVH deploys its own fiber optic network across the globe.
- The OVH network comes with a bandwidth capacity of 4.5 Tbps in Europe and 8000 Gbps in North America

Hosting partner premises (2/2)

❑ Resources

- All elements of the infrastructure are dedicated to Rainbow
  - No resources shared with other company
  - Raw hardware / raw network / storage resources provided
  - OVH Monitors handles and operates all raw resources

- OVH provides multiple world-wide Point of Presence (PoP) (in UE, NA, AS and OC)

OVH Anti DDoS

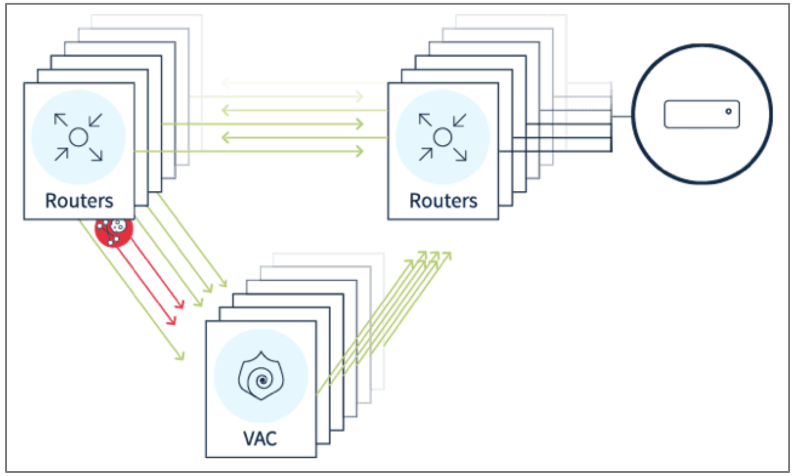
Anti-DDoS (1/3)

❑ 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



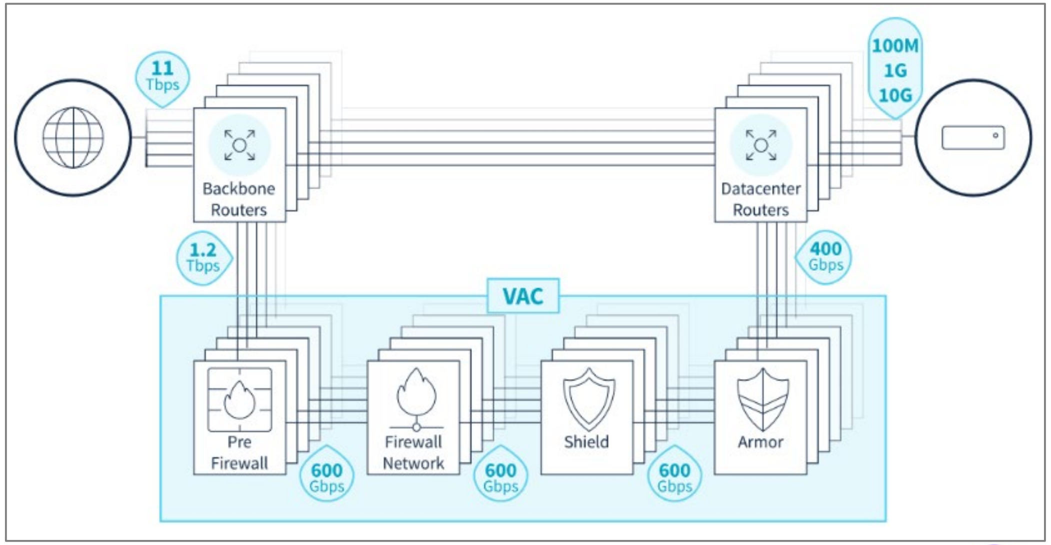
❑ It is seen as a black box in which filters are not disclosed for security reasons.

❑ It's hardware ASIC-based packet filtering equipment.

Anti-DDoS (2/3)

❑ The VAC processes occur in four steps

- pre-firewall
  - It is fully managed by OVH, and applies rules that define filters directing data packets to the Firewall Network
- 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.
- 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.
- Armor
  - Armor is the most advanced filter in the VAC, and intervenes in mitigating the strongest attacks.



Anti-DDoS (3/3)

❑ The VAC solution is replicated in 10 data centers spread on 3 continents.

- Total capacity of more than 4 Tbit/s.
- Analysis of incoming traffic, 1s detection, 4Tb/s capacity
- Under attack, the traffic is diverted and illegetimate packets are discarded
- 1 ms additional delay in case of DDoS mitigation

❑ For Rainbow:

- All Rainbow servers are behind OVH’s Anti-DDos firewall
- 3x 160 Gbps anti-DDoS infrastructures have been set up.

Refer to OVH web site for more information on anti-DDoS: OVH Anti-DDOS technology

OVH Certificates and compliance

Certificates

❑ Our Cloud Service Provider (OVH) has at the following security certifications:

- PCI-DSS
- STAR self-assessment
- ISO/IEC 27001
- HDS approval (Health Data Hosting)
- SOC certified technologies
  - SOC 1 type II (SSAE 16 / ISAE 3402 (formerly SAS 70))
  - SOC 2 type II
  - SOC 3

ARCHITECTURE LEVEL SECURITY

Rainbow regions breakdown (1/2)

❑ The global Rainbow architecture is distributed geographically on 5 regions isolated in terms of data storage but inter-connected through a federated network:

- Europe Middle-East and Africa (EMEA),
- Germany,
- North America (NA),
- Caribbean and Latin America (CALA),
- Asia-Pacific (APAC).

❑ Mainland China is the 6th region completely isolated from the global Rainbow network

- No possible link with rest of the world.

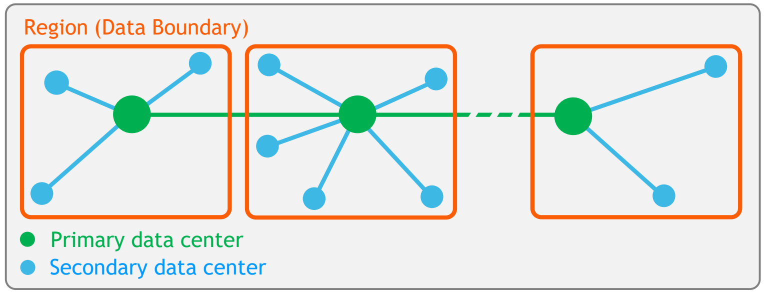
Rainbow regions breakdown (2/2)

❑ The objective is to:

- Offload the network infrastructure
  - by providing Rainbow's users direct local access to static resources through an IP AnyCast mechanism (CDN: Content Delivery Network) .
- Provide the best user experience
  - Service latencies are minimized
- Ensure data privacy at regional level
  - Comply with legal regulation
  - Sensitive data are not replicated across boundaries

Data Centers

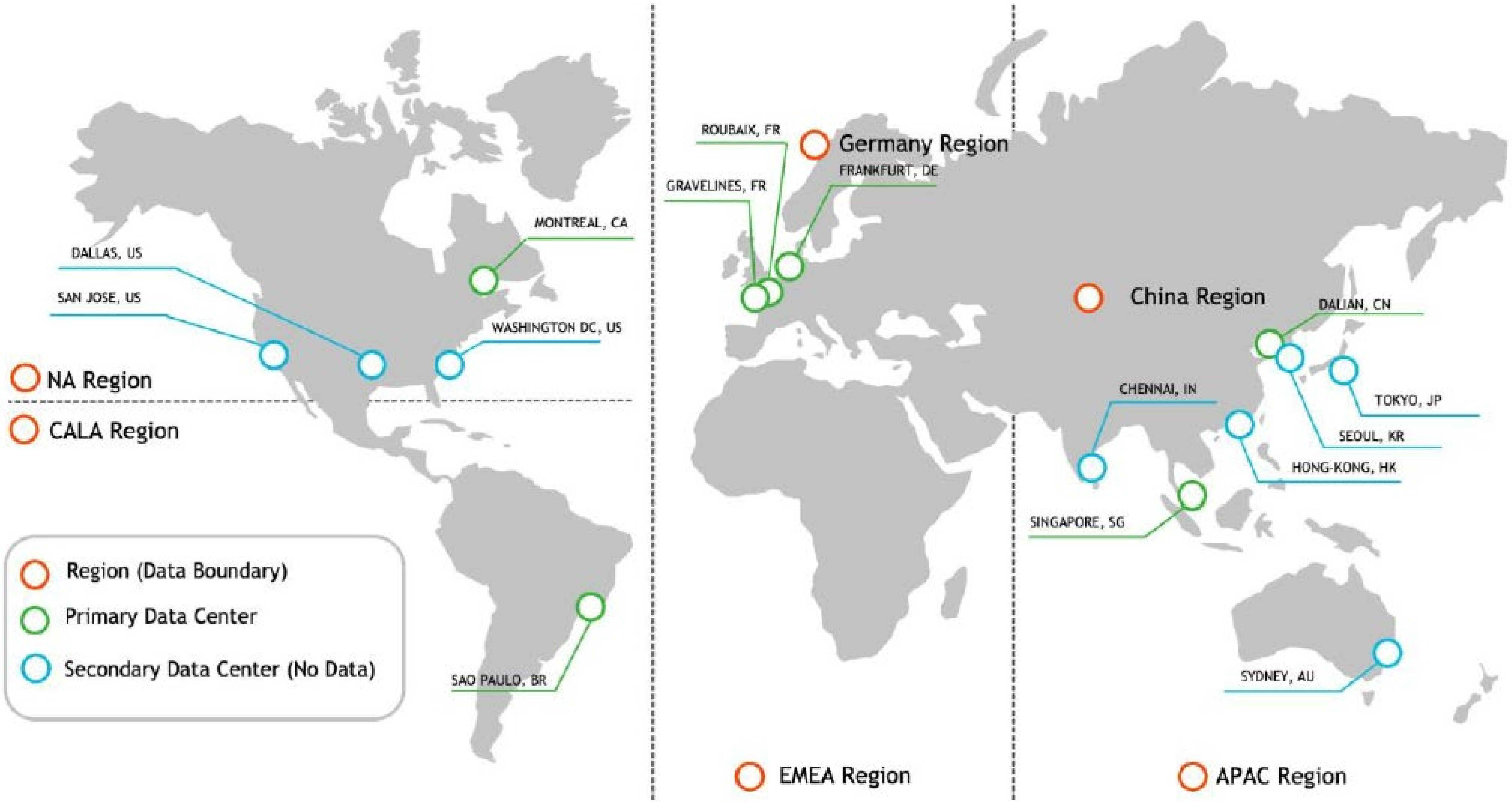
- ❑ ALE has deployed two categories of data centers:
  - ▪ Primary data centers which store data
  - ▪ Secondary data centers which don't store data



- ❑ A media relay server (TURN server) is operated in each data center.

Data Center Localizations	
Primary Data Centers	Secondary Data Centers
Gravelines and Roubaix (EMEA, France), OVH	Dallas, San Jose and Washington (US) , IBM
Frankfurt (EMEA, Germany), OVH	Chennai (IN) , IBM
Montreal (NA, Canada), OVH	Hong-Kong (HK) , IBM
Singapore (AS), OVH	Seoul (KR) , IBM
Sao Paulo (CALA, Brazil), IBM	Tokyo (JP), IBM
Dalian (CN), Neusoft	Sydney (AU), OVH

Geographical repartition



Healthcare specificity

❑ In addition to the standard Rainbow instance mentioned previously, there is a specific instance dedicated for hosting sensitive healthcare data.

- Hosted in a dedicated HDS data center,
- Localized in France,
- Compliant with French healthcare regulation - HDS certification,
- Companies outside France can benefit of this Rainbow instance dedicated to healthcare,
- The HDS rainbow instance is isolated from the standard rainbow instance.

❑ "HDS" option is declared by the ALE super-administrator at the Rainbow company creation

- No possible migration from an existing company created in the generic offer,
- All users of a company with HDS option will benefit from the healthcare dedicated environment hosting,
- Rainbow HDS is dedicated to healthcare companies only.

Refer to the document "Rainbow HC Security" for additional information

USER LEVEL SECURITY

User access

User authentication (1/3)

❑ Rainbow offers different possibilities to authenticate users

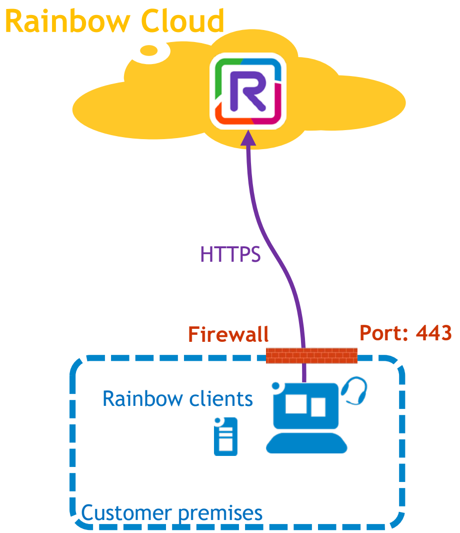
- **Internal**
  - Let Rainbow completely manage the login /password security rules.
  - Under control of the Rainbow administrator.
  - Nothing to configure, it’s the default solution.

- **External authentication**
  - 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)

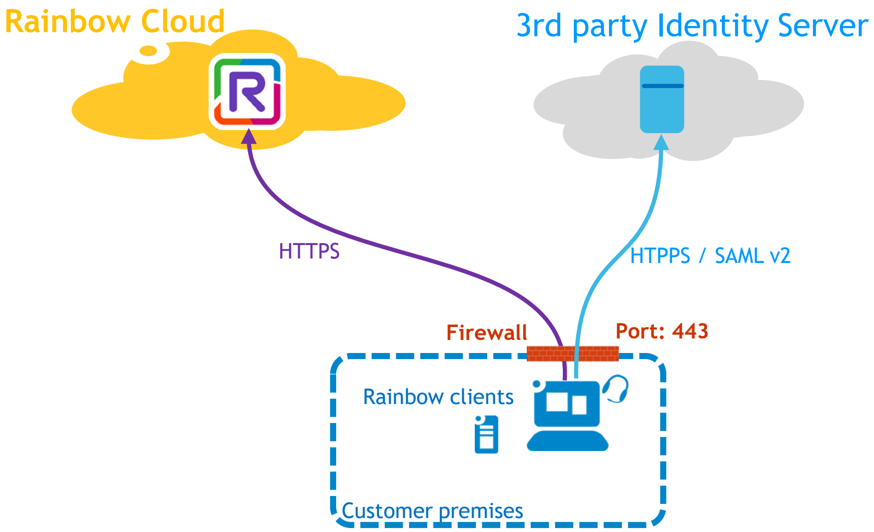
User authentication (2/3)

❑ Topologies and flows

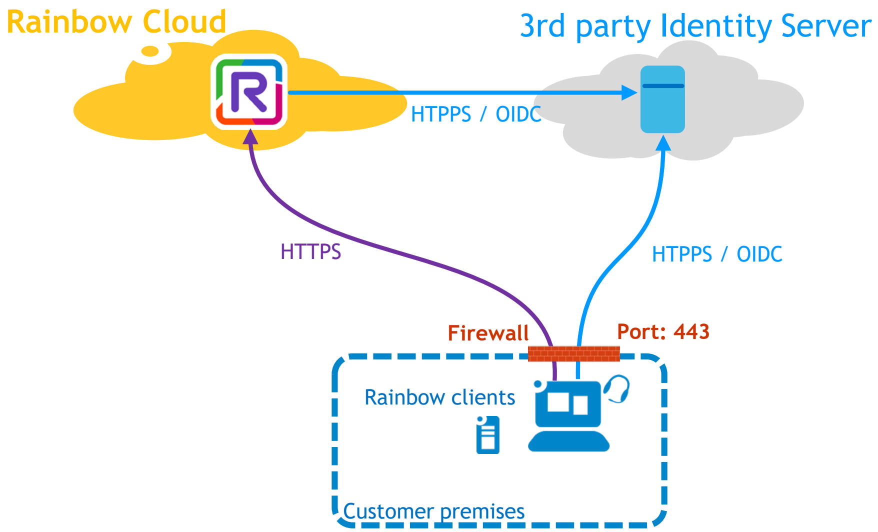
Internal authentication



External authentication with SAML v2



External authentication with OIDC



User authentication (3/3)

❑ 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.

Email & Domain name

❑ A Rainbow user uniquely identified by his email address can belong to one company only.

❑ Control on the “login” domain name

▪ To avoid dishonest domain name appropriation, only Rainbow ALE super-administrator can configure domain names for companies.

▪ Several domain names can be defined per company.

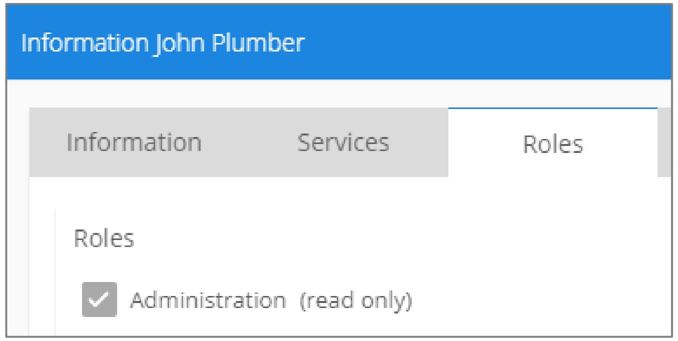
▪ New Rainbow users having an email domain names corresponding to company’s one are automatically linked to this company.

  • This concerns user self-registrations in Rainbow.

User role

User roles (1/3)

- Rainbow users in an End Customer company may have one of the two following roles:
  - As a simple **User**
    - Access to the Rainbow features will depend on his Rainbow subscription.
      - Essential/Business/Enterprise, Monthly or Prepaid
  - As a Company **Admin**
    - Additionally to the rights of the simple **User**, he can administrate his company.



Information John Plumber

Roles

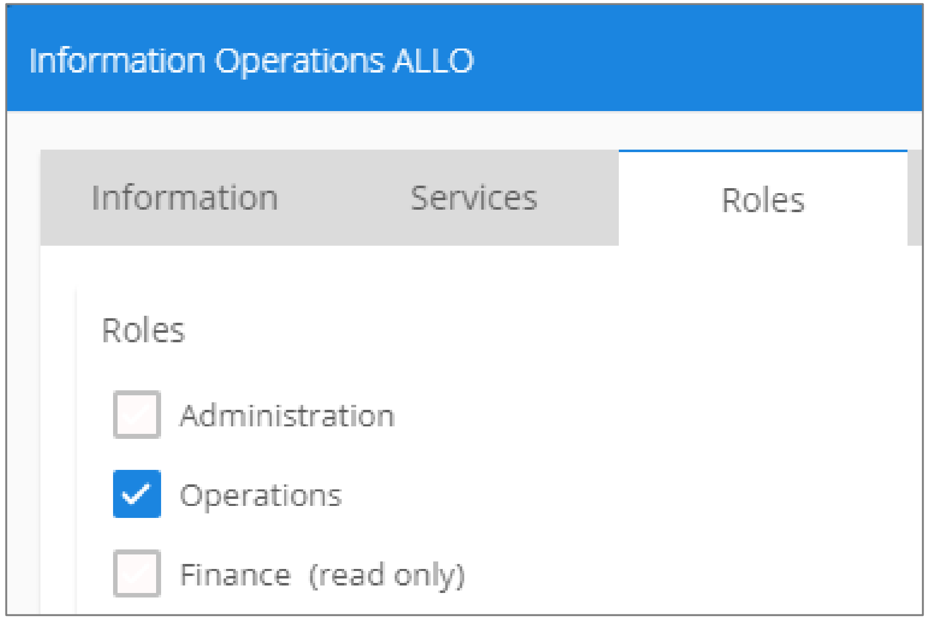
☑ Administration (read only)

- Without being a **Rainbow User**, a person can be invited in a conference (Bubble)
  - In that case, as member of the conference, he benefits of a **Guest** role.
  - Has access to IM, file sharing, desktop sharing, audio and video features during a conference only.
  - Invited by email with a conference link access (URL).

User roles (2/3)

❑ For Business Partners only, there are two additional user roles permitting to administrate their customers:

- **Finance role** provides the following rights:
  - Create company and his members,
  - Create and manage subscriptions,
  - Assign licenses to the company members,
    - Essential/Business/Enterprise, Monthly or Prepaid
  - Check invoices.
- **Operation role** provides the following rights:
  - Create company and his members,
  - Assign licenses to the company members,
    - Essential/Business/Enterprise, Monthly or Prepaid
  - Connection to on premises equipment (OXE, OXO, third-party-pbx, WebRTC gateway).
  - Associate PBX extensions with Rainbow user accounts.


Information Operations ALLO

Roles

☐ Administration

☑ Operations

☐ Finance (read only)

For additional information refer to: [What is the Finance Role?](#)
[What is the Operation Role?](#)

User roles (3/3)

❑ Rights depending on the user’s role

- Related to company management

		Create/Manage Company *(Info/Members invitation)*		**Create Equipment** *(Add Systems)*		**Manage Systems** *(User/Device association)*	
	Roles	BP company	EC company	BP company	EC company	BP company	EC company
Business Partner (BP)	Operation	YES	YES	YES	YES	YES	YES
	Finance	YES	YES	NO	NO	NO	NO
	Admin	YES	NO	YES	NO	YES	NO
End Customer (EC)	Admin		YES		NO		YES

- Related to subscription management

		Create subscriptions		**Manage subscriptions**		**License allocation**	
	Roles	BP company	EC company	BP company	EC company	BP company	EC company
Business Partner (BP)	Operation	NO	NO	With rights*	NO	YES	YES
	Finance	YES	YES	YES	YES	YES	YES
	Admin	YES	NO	YES	NO	YES	YES
End Customer (EC)	Admin		YES		With rights*		YES

Finance Role: Only for Business Partner
Operation Role: Only for Business Partner
Company Administrator: for both Business Partner an End Customer

With rights *: if the Finance Role is assigned to the Admin

Company confidentiality

Company visibility (1/6)

❑ In order to preserve the confidentiality, there are four company visibility modes permitting to adjust how company's members are reachable:

- Public, Private, Closed and Isolated

❑ By default, company visibility mode is set to "**public**"

❑ By default company's members inherit the visibility mode of their company but it can be personalized by the administrator for each member.

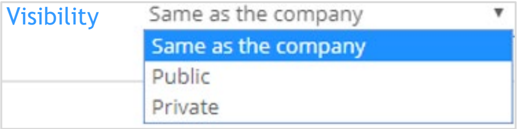
❑ The visibility mode affects directly capabilities on:

- The Rainbow search engine 🔎
- The Rainbow contact invitation ✉

Company visibility (2/6)

- User visibility mode depending on the company visibility mode

Company visibility mode	Members default visibility mode inherite from the company	Possible derogatory visibility mode for selected members
PUBLIC	PUBLIC	PRIVATE
PRIVATE	PRIVATE	PUBLIC
CLOSED	CLOSED	PUBLIC PRIVATE
ISOLATED	ISOLATED	PUBLIC PRIVATE

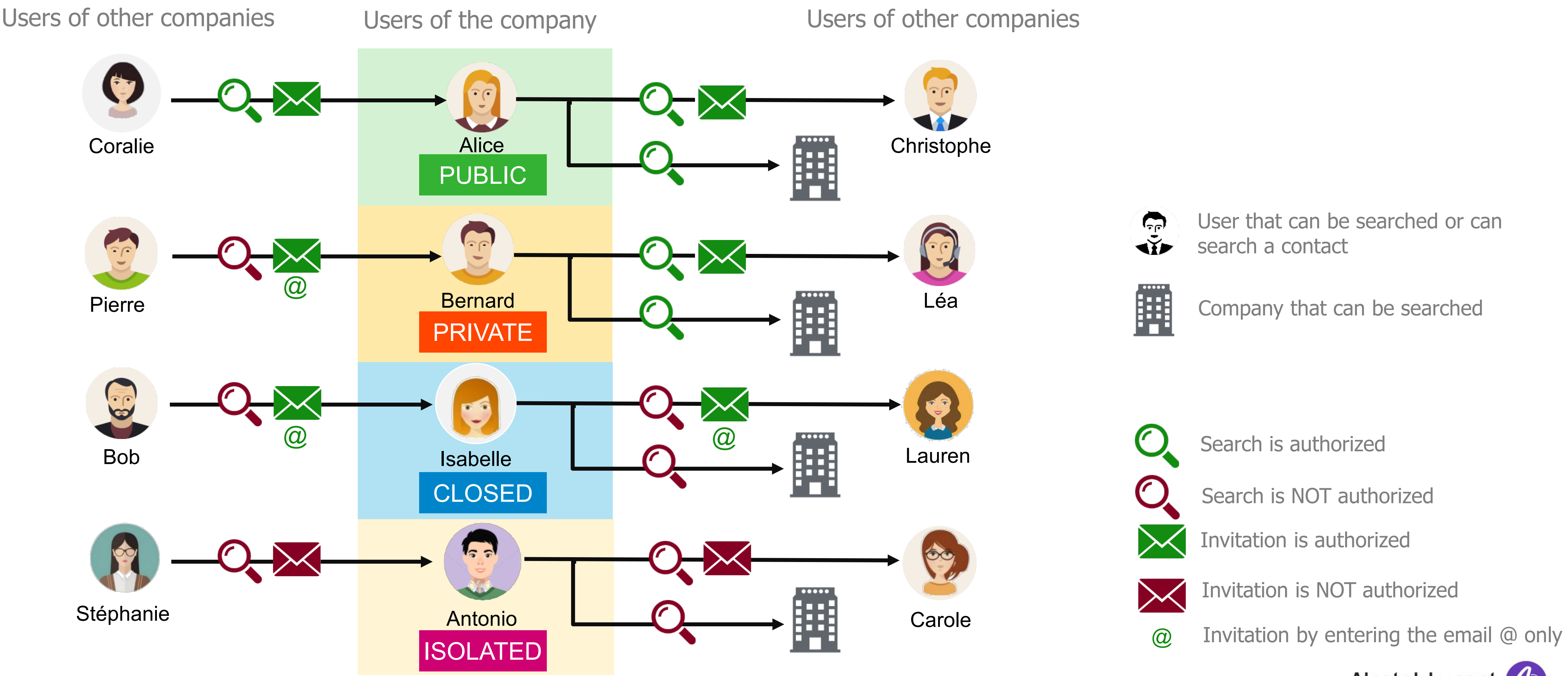


Visibility: Same as the company ▾

- Same as the company
- Public
- Private

Company visibility (3/6)

❑ Four company visibility modes



Users of other companies

Users of the company

Users of other companies

Coralie

Alice

PUBLIC

Christophe

Pierre

Bernard

PRIVATE

Léa

Bob

Isabelle

CLOSED

Lauren

Stéphanie

Antonio

ISOLATED

Carole

User that can be searched or can search a contact

Company that can be searched

Search is authorized

Search is NOT authorized

Invitation is authorized

Invitation is NOT authorized

@ Invitation by entering the email @ only

Company visibility (4/6)

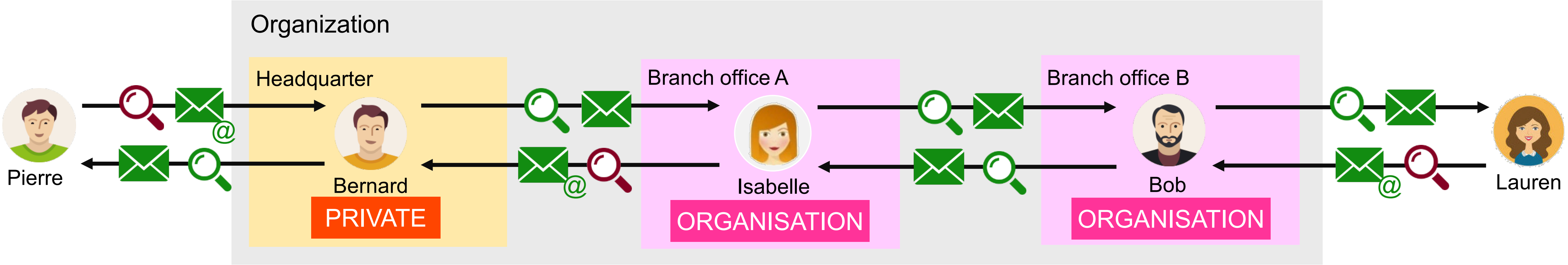
- ❑ Complementing the four company visibility modes there is an “**Organization**” visibility mode:
  - ▪ This visibility mode is only accessible to the company’s administrator when his company belongs to an organization.
  - ▪ An “**Organization**” company is seen as a “**Private**” company for users outside the organization.
    - Members can search and invite contacts outside the company and be invited by users of other companies (identical to private mode)

- ❑ Rules between companies in the same organization are particular:
  - ▪ Members belonging to different “**Organization**” companies are seen as if they were in the same company.
  - ▪ Members of “**Organization**” companies CANNOT search members in a “**Private**” company.
  - ▪ Members of a “**Private**” company can search members of “**Organization**” companies.

Company visibility (5/6)

❑ Typical use case is an organization with a headquarter and several branch offices:

- The headquarter has the “**Private**” visibility mode.
- The branch offices have the “**Organization**” visibility mode.



❑ Particularity:

- Companies/users in an organization with the visibility mode “**Closed** “ or “**Isolated**” are seen as:
  - public inside the organization,
  - and with their classical respective behaviors from outside the organization.

Company visibility (6/6)

❑ In addition to the fifth visibility modes which can be set up by the company administrator, there is the “**Visibility by**” feature:

- Enables two private companies' users to see on other.
- Only accessible to ALE Rainbow Super-Administrator.
  - The request must be done to Rainbow support
- Whatever the visibility mode the “Visibility by” feature can be applied.

User network

- ❑ Contacts in the user’s network are referenced in a Rainbow search engine.
  - ▪ This means that a contact from another company in private mode can be seen if this one belong to the user’s network.

- ❑ Presence status of a contact can be seen by a user only if the contact belong to the user’s network
  - ▪ Requires an invitation to the contact to be part of the user’s network
  - ▪ Invitation automatically accepted when the contact is in the same company
  - ▪ Invitation must be accepted by the contact if he is in a different company
    - Always possible to revoke later an accepted invitation

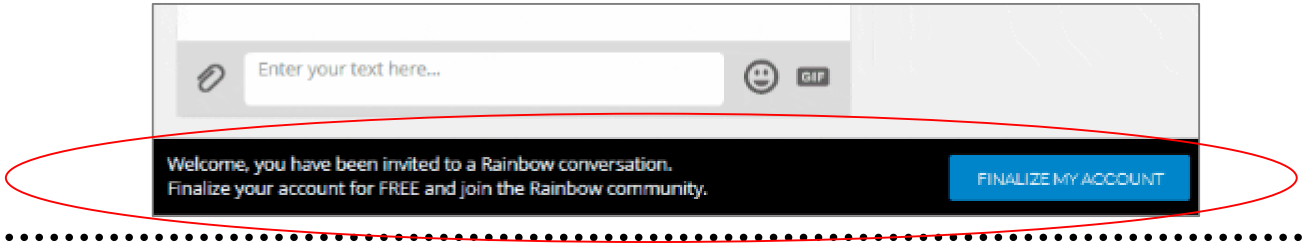
- ❑ Favorites are seen as contacts in the user’s network. So, they are also referenced in the Rainbow search engine.

Multi-media conference access

Bubble - Roles for members

❑ Participants in a Bubble (Multimedia conference) may have different roles:

- **Organizer** (or **Owner**)
  - The organizer is the creator of the bubble and is unique.
  - He has the entire controls to manage the bubble.
- **Co-organizer**
  - He is a member which has been promoted as co-organizer by the owner of the bubble.
  - He inherits rights for specific actions to animate the conference.
- **Member**
  - He is a person who has been invited as a simple participant.
  - He may already be a **Rainbow user** or not be **Rainbow user** yet.
    - A **non Rainbow user** has a '**guest**' role and received automatically the invitation by email.
    - It's not necessary for a guest to have a Rainbow account to participate to the multimedia conference (bubble).
      - However, the user interface will suggest him to create his Rainbow account.



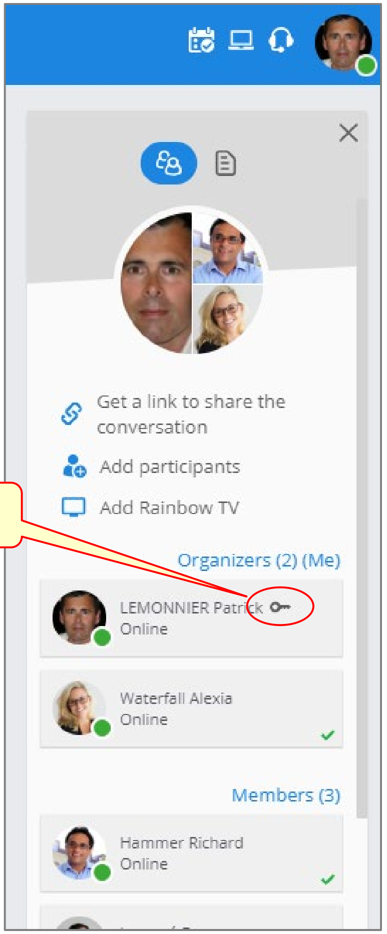
Welcome, you have been invited to a Rainbow conversation.
Finalize your account for FREE and join the Rainbow community.

Bubble - Ownership transfer

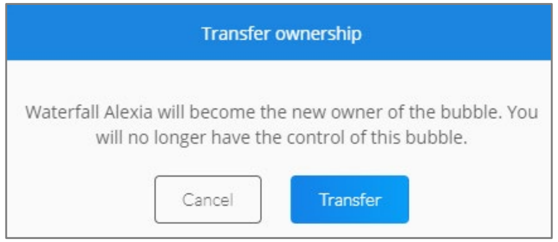
- ❑ Owner (or Organizer) of a Bubble may not have the responsibility anymore (activity transfer, left the company).

- ❑ In order to preserve the Bubble and its contain, the ownership of a bubble can be transferred:
  - First, the future owner must be promoted as co-organizer
  - Then, the ownership can be transferred to the co-organizer

For additional information refer to: [How to assign roles to bubble members]()



Owner of the Bubble



Transfer ownership

Waterfall Alexia will become the new owner of the bubble. You will no longer have the control of this bubble.

Bubble - Conference access and possible actions

❑ Audio/Video conference access is restricted

- At least one conference organizer or co-organizer already in the conference to authorize the entry of simple participants.
- Only invitees can participate to the conference.

❑ Depending on their role, the participants will have some action rights on the conference.

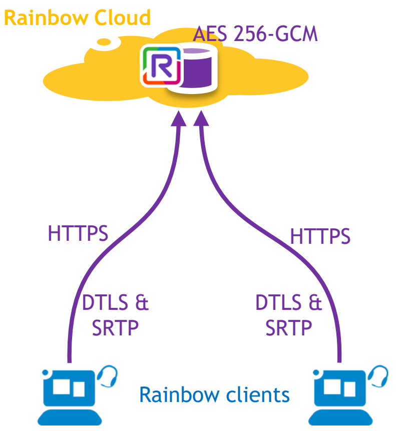
	Roles	Actions						
		Delete bubble	Archive bubble	Ownership transfer	Get conference link	Promote to Co-organizer	Add / Remove participant	Start conference
Bubble participant	Member	NO	NO	NO	NO	NO	NO	NO
	Co-organizer	NO	NO	NO	NO	YES	YES	YES
	Organizer	YES	YES	YES	YES	YES	YES	YES

DATA LEVEL SECURITY

User data

Data protection

- ❑ End-user passwords are hashed and salted in Rainbow’s internal database.
  - based on SHA256 for HMAC with 4096 iterations



- ❑ All data (IMs, files) exchanged between users or through bubbles are encrypted <u>in transit</u> and <u>at rest</u>.
  - For transit, HTTPS + WSS through TLS 1.2/1.3 only
  - At rest, AES 256-GCM is used

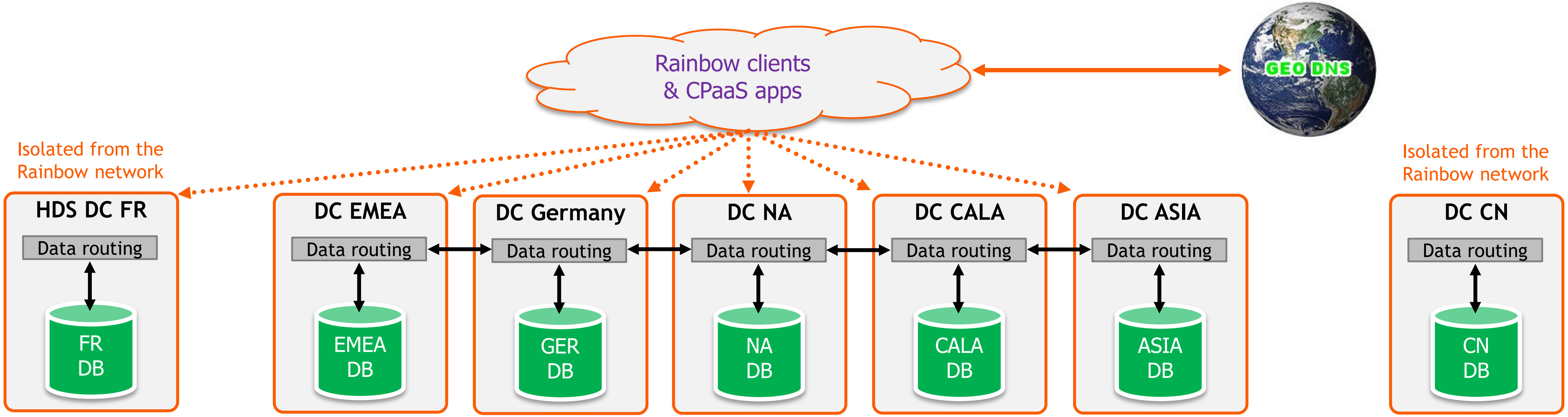
- ❑ Voice/Video communications are natively encrypted using WebRTC technology using DTLS & SRTP.

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

Data residency

- ❑ Company’s data are located in the data center of the company’s region.
  - ▪ Their users data are then also stored in the same data center.

- ❑ Worldwide standalone users are automatically affected to the default company which is “Rainbow”.
  - ▪ The “Rainbow” company is located in France in the EMEA data center.



Data Availability

- ❑ To ensure data high availability, different mechanisms are in place:
  - Hardware level with HA disk (OVH responsibility)
  - 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
    - Retention of the daily backup is one week
  - 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, IBM).

Data restriction

- ❑ In order to control file exchanges between users, it’s 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.

- ❑ As a protection against usurpation, it’s possible to forbid the modification by user of his title, first name and last name.

Activity data

Activity logs

- ❑ All user requests to the Rainbow application are logged
  - ▪ Including all administrators activities.

- ❑ Logs are:
  - ▪ completely anonymized.
  - ▪ sent to a cluster of servers where they are stored redundantly.
  - ▪ kept during the minimal duration imposed by law.
    - Activity logs kept 12 months following the French law (not technical logs)
  - ▪ stored in a database located in the region where they are produced.
  - ▪ accessible only by ALE Rainbow operation team members.
    - <u>No password nor any conversation </u>are visible in logs.

Logs analysis

Rainbow™

- ❑ 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 don’t 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 users identity,
  - The data and time of the requests,
  - The type of the requests.
- ❑ Logs analysis **never permits** to retrieve:
  - The conversations,
  - The passwords.

Data deletion

Data deletion
User account categories

❑ Deletion of data depend on the category of the user accounts

- Standalone user accounts:
  - They don’t belong to a company
  - Users fully manage their account
  - RGDP rules applied are directly under the responsibility of ALE Rainbow team

- User accounts attached to a company
  - Users can manage their profile if they have rights.
  - Users account are fully controlled by the company’s administrators (or by delegation by the Business Partner)
  - RGDP rules applied are still under the responsibility of ALE Rainbow team but company’s administrators are also implied on some aspects.

Data deletion
Standalone user accounts

❑ Users are fully owner of their accounts

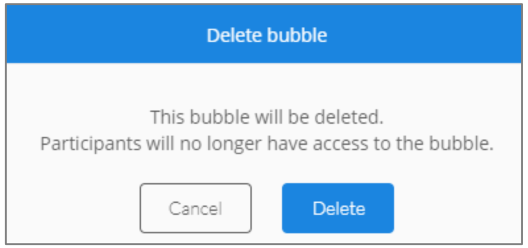
- Daily
  - In an IM conversation a user can delete his last sent message and any file he has attached in the conversation flow.
  - The owner of a bubble can suppress it as he wants.
    - All participants will no more have access to this bubble.
    - Instead, he can also choose to archived his bubble before to delete it definitively.

- At T0, users can delete themselves their accounts
  - User's account his closed, no more login is possible
  - Profile data remain visible for 1 month (IM , files, bubbles)
  - The user is still visible by others
- At T+30 days, user's profile is automatically anonymized
  - Other users in relation with the closed account see a terminated account with *** replacing the user name.
  - Files are deleted
  - Bubbles are archived, no more participant in any bubbles
- At T+ 60 days, deletion of remaining user's data

Data deletion
User accounts attached to a company

❑ Deletion at the user level

- In an IM conversation a user can delete his last sent message and any file he has attached in the conversation flow.
- The owner of a bubble can suppress it as he wants.
  - All participants will no more have access to this bubble.
  - Instead, he can also choose to archived his bubble before to delete it definitively.
- A user cannot suppress his account himself.


Delete bubble

This bubble will be deleted.
Participants will no longer have access to the bubble.

❑ Deletion at the administrator level (Business Partner or Customer)

- Can delete a user accounts
- At T0, the user’s account his closed, no more login is possible
  - Profile data remain visible for 1 month (IM , files, bubbles)
  - The user is still visible by others
- At T+30 days, user’s profile is anonymized
  - Other users in relation with the closed account see a terminated account with *** replacing the user name.
  - Files are not deleted (files belongs to the company)

SMTP server

SMTP server

❑ Rainbow implements its own SMTP server: Postfix.

❑ Emails sent through this SMTP server are generated by Rainbow services only.

- This means that end users or administrators in Rainbow cannot send emails through this email server.

❑ This SMTP server is used for the following tasks:

- Account confirmation at the creation
- Password renewal
- Invitation of external guests to a conference
- Send conversation into the user email box

❑ By restricting the access to the SMTP server to Rainbow services, this one is then protected against any fraudulent usage.

❑ In order to permit the authentication of emails and his sender (Rainbow services), the following technologies:

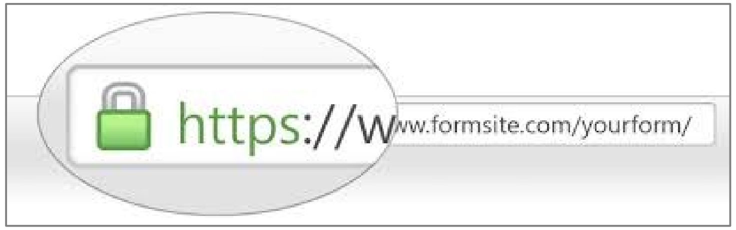
- SPF (Sender Policy Framework), DKIM (Domain Key Identified Mail),
- DMARC (Domain-based Message Authentication, Reporting and Conformance),
- and BIMI (Brand Indicators for Message Identification).

TRANSPORT LAYER SECURITY

Rainbow SSL/TLS Policy (1/2)

- 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



https://www.formsite.com/yourform/

- 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
  - Don’t offer deprecated weak SSL support.
  - Every HTTPS negotiation is done through TLS only

Rainbow SSL/TLS Policy (2/2)

❑ 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.

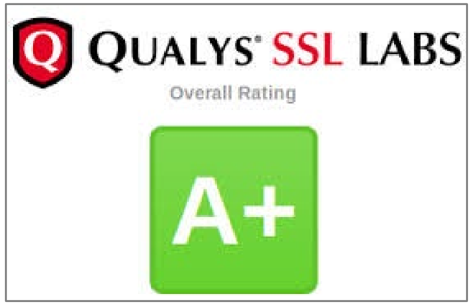
SECURITY AUDITING

Security auditing (1/2)

❑ The Rainbow infrastructure and software solution are under constant scrutiny using different tools:

- Nmap,
  - A tool used to track opened ports
- Tenable.io Vunerability management (ex Nessus cloud),
  - An online vulnerability scanner permitting to highlight weaknesses on a network or a system.
- Qualys SSL Labs
  - An online test to audit the quality of the SSL certificate of the Web sites.
  - Rainbow is ranked A+ by Qualys SSL Labs security test:

For more information refer to: Qualys SSL Labs


QUALYS® SSL LABS

Overall Rating

A+

Security auditing (2/2)

❑ The Rainbow solution is audited each year by external independent actors:

- CGI Business Consulting (March 2017, July 2018)
- Orange Cyber Defense (January 2017, August 2017, August 2019)

❑ All necessary actions are taken by ALE Rainbow teams to mitigate or eliminate the discovered threats.

CERTIFICATION AND COMPLIANCE

ALE Certifications

❑ Certifications

- ISO/IEC 9001
- ALE (including Rainbow) is certified ISO/IEC 27001:2013 (certificate received in March 2019)
- ISO/IEC 27017/27018 for Rainbow planned for 2020

❑ Data protection

- GDPR Compliance

❑ Compliance for healthcare market

- Rainbow is certified HDS (certificate received in October 2019)
  - follows French health public legal framework laid down in article L1111-8.

Conclusion

Documents

- ❑ Hereafter, the list of the external information sources referenced in this document:
  - Rainbow - Solution Brief – Security Abstract
  - How to assign roles to bubble members
  - What is the Finance Role
  - What is the Operation Role
  - Rainbow HC Security
  - Qualys SSL Labs
  - OVH Anti-DDOS technology

Conclusion

❑ All security elements are operational in standard whatever the chosen subscription.

❑ Except HDS option which benefits additionally a dedicated and isolated hosted environment respecting additional specific rules.

- A request to the ALE Rainbow team must be done.

Follow us on:

Twitter.com/ALUEnterprise

Facebook.com/ALUEnterprise

Youtube.com/user/enterpriseALU

Linkedin.com – Group: Alcatel-Lucent Enterprise

Slideshare.net/tagged/Enterprise

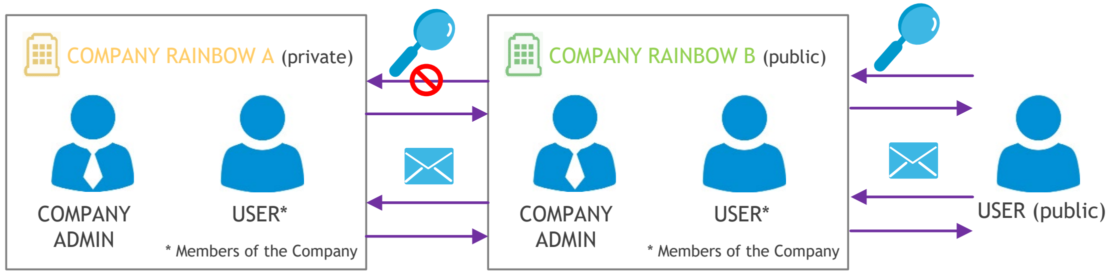
Storify.com/ALUEnterprise

Company visibility

❑ Four company visibility modes

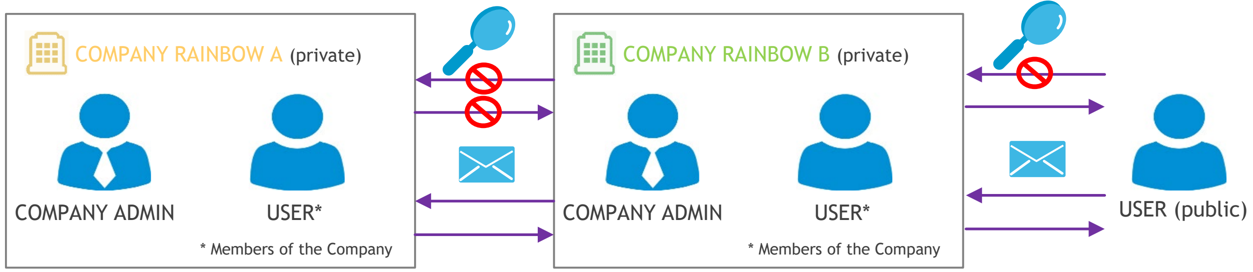
Public company

- Members of a public company are referenced in the Rainbow search engine of other companies.
- Company's public pages are referenced in the Rainbow search engine.
- Enables concrete inter-enterprise collaboration.



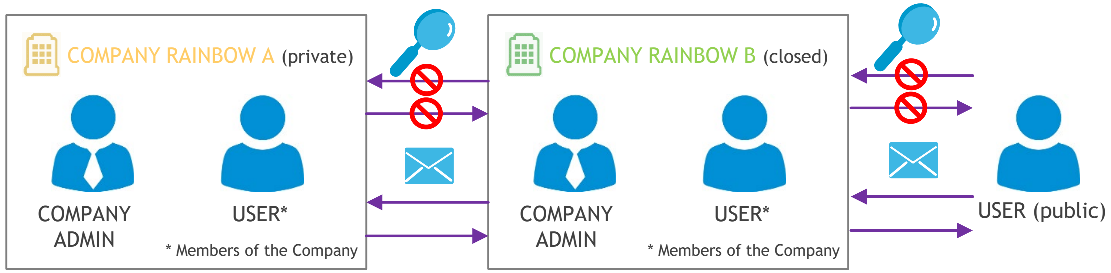
Private company

- Rainbow search engine does not retrieve information of private company (to users who are not members).
- Company's public pages are visible to members ONLY through the search engine.
- Members can join the network of another company's user ONLY by the mechanism of email invitation.



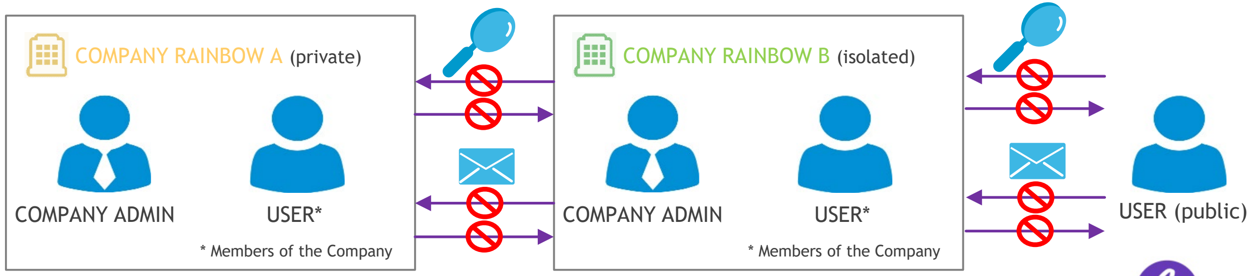
Closed company

- A closed company is seen as private
- Members can join the network of another company's user ONLY by the mechanism of email invitation.
- Members can invite other companies' users.



Isolated company

- A isolated company is seen as private
- Members CANNOT join the network of another company's user by the mechanism of email invitation.
- Members CANNOT invite other companies' users.



enterprise.alcatel-lucent.com

End