RAINBOW™ EDGE par ALCATEL-LUCENT ENTERPRISE

ANSSI Cible - CSPN Ed 1.3.1

JANVIER 2023

Reference - OD-405320

Alcatel·Lucent Enterprise

Contenu

Glossaire

ALE: Alcatel-Lucent Enterprise

PBX: Private Branch Exchange

ICE: Interactive Connectivity Establishment – RFC 5245

STUN: Simple Traversal of UDP through NAT – RFC 5389

TURN: Traversal Using Relays around NAT – RFC 5766

1 Introduction

1.1 Objet du document

Ce document concerne le service de collaboration Alcatel-Lucent Rainbow délivré par Alcatel-Lucent Enterprise (ALE) qui assure des communications sécurisées a ses clients.

Ce document définit la cible de sécurité visée dans le cadre de l'évaluation de Certification de Sécurité Premier Niveau (CSPN) dans un contexte *Cloud Computing* ou informatique en nuage.

1.2 Identification du produit

Société	**Alcatel-Lucent Enterprise**
Nom du produit	Logiciel Multi-tenant **RAINBOW™ EDGE PAR ALCATEL-LUCENT ENTERPRISE** en tant que service Saas version en hébergement cloud privé sur socle IaaS
Lien	**https://www.openrainbow.com**
Numéro de version évaluée	**Version solution 114** **client Web 2.114.x**
Catégorie de produit	**Communication sécurisée**

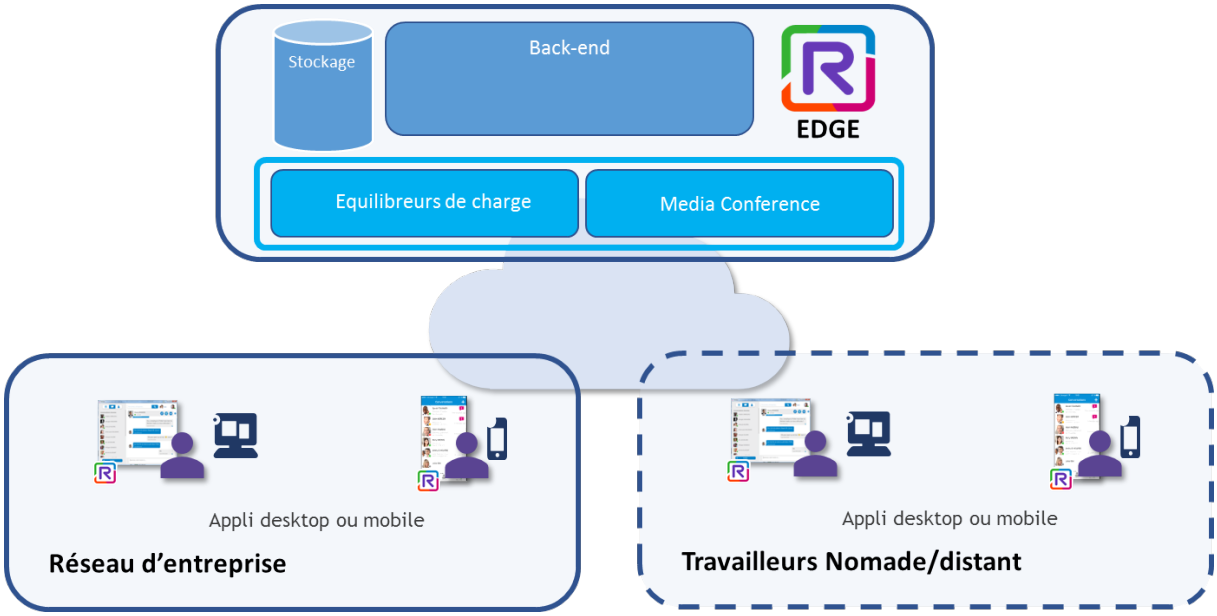
Pour Windows et MAC, la version visible au niveau des fichiers de l'OS est celle du conteneur qui n'agit qu'en hébergeur de l'application. La véritable application portant le fonctionnel et les fonctions de sécurité présente sa version dans la fenêtre « A propos de Rainbow »

2 Description du produit

2.1 Description générale

Le service de collaboration Rainbow dans sa version Rainbow EDGE est hébergé sur un cloud privé ou dans un data center. Il est installé et maintenu par Alcatel-Lucent Enterprise. Il fournit à ses clients un service de collaboration avancé et sécurisé leur permettant de communiquer en voix, vidéo ou messages. Ces communications peuvent être point à point ou multipoints. Les données échangées peuvent avoir différents formats : images, vidéo, texte, partage d'écran. Des fichiers peuvent aussi être échangés au cours de ces communication, ils sont alors conservés dans un espace de stockage intégré au service.

Les abonnés au service Rainbow utilisent une application client Rainbow déployée sur leur ordinateur et/ou sur leur téléphone mobile. Cette application client établit des flux d'échange avec le serveur Rainbow.



2.2 Description de l'utilisation du produit

Le service de collaboration Rainbow utilisé dans un contexte professionnel est géré par des partenaires revendeurs d'Alcatel-Lucent Entreprise agissant en tant que prestataires de service. Ces revendeurs sont créés par Alcatel-Lucent Entreprise et identifiés par le service Rainbow au travers d'une procédure d'authentification lors du lancement de l'application client Rainbow. Ces partenaires créent le contexte de définition d'une nouvelle entreprise abonnée au service Rainbow et la liste de ses employés pour les bénéficiaires.

Les utilisateurs bénéficiaires d'une nouvelle entreprise reçoivent un mail initial qui les invitent à se connecter sur l'application cliente Rainbow et à compléter leur profil utilisateur en particulier en choisissant un mot de passe personnalisé. Il leur est proposé d'installer une version de l'application client Rainbow propre au système d'exploitation de leur ordinateur ou de leur téléphone mobile.

Par la suite, quelle que soit l'application cliente Rainbow utilisée, l'utilisateur bénéficiaire devra s'authentifier avec son adresse mail et le mot de passe qu'il a choisi. Il pourra alors établir des communications point à point ou multipoints avec d'autres utilisateurs du service Rainbow. Ces communications pourront être sous forme d'échange de messages, voire de fichiers ou au moyen de flux de média audio et/ou vidéo. Les sources des flux sont les ressources matérielles (caméra, micros, …) de l'ordinateur ou du téléphone mobile plus un partage possible de l'écran de l'utilisateur.

Tous les flux établis entre une application client Rainbow et le service Rainbow coté serveur sont chiffrés. De même, les flux directement établis en point à point entre deux applications client Rainbow, sont chiffrés.

2.3 Description de l'environnement

L'application client Rainbow est disponible sur PC, Mac, iOS **et** Android.

Les versions de système d'exploitation supportées sont consultables dans un document sur le site de support de Rainbow.

Liste officielle des fonctionnalités (onglet application – section software requirements)

Au moment de la rédaction de ce document, on y trouve :

Operating systems	
Microsoft Windows 7 Microsoft Windows 8.1 Microsoft Windows 10 Microsoft Windows 11	Windows Operating System supportés. Toutes editions sauf RT 32/ 64-bit.
Apple macOS 10.13 (High Sierra) Apple macOS 10.14 (Mojave) Apple macOS 10.15 (Catalina) Apple macOS 11 (Big Sur) Apple macOS 12 (Monterey)	Apple Operating System pour ordinateur. Versions 10.11 (El Capitan) and 10.12 (Sierra) ne sont plus supportés.
Chrome OS	Pour ordinateur et autre matériel compatible.
Apple iOS 13 Apple iOS 14 Apple iOS 15	Pour iPhone et iPad

Google Android OS 8.0 (Oreo) Google Android OS 9.0 (Pie) Google Android OS 10 Google Android OS 11 Google Android OS 12	Google Operating System pour smartphones Android.

2.4 Description des hypothèses sur l'environnement

On distingue l'environnement d'hébergement du service Rainbow coté serveur de l'environnement client ou s'exécute l'application client Rainbow.

2.4.1 Utilisateurs type

Chaque bénéficiaire du service Rainbow est d'abord authentifié puis se voit attribuer un niveau de fonctionnalités qu'il peut utiliser. Ainsi un partenaire prestataire d'Alcatel-Lucent Enterprise aura des droits de gestion des compagnies clientes qui ne seront pas accessibles ou seront réduits s'il est un simple employé d'une compagnie abonnée au service. Cette notion de compagnie crée une notion de cloisonnement pour le groupe de bénéficiaires qui lui est rattaché.

On distingue les acteurs qui ont des rôles d'administrations et les acteurs utilisateurs du service de communication Rainbow. Il est possible pour un acteur administratif d'utiliser aussi la partie communication.

Parmi les acteurs administratifs, on trouve :

- L'organisation Opération d'ALE chargée du déploiement et de la maintenance du service hébergé
- Les partenaires d'ALE enregistrés et contractualisés par ALE qui sont amenés à revendre le service à des entreprises pour lesquelles ils assurent une configuration initiale et une maintenance évolutive du service Rainbow. Les partenaires n'ont pas à gérer l'installation de logiciel dans la partie hébergée. Ils peuvent fournir un service de déploiement des applications client Rainbow ou au minimum en assurer le support
- Les clients finaux avec une délégation d'administration, employés d'une entreprise abonnée au service Rainbow, ils assurent des fonctions de personnalisation du service au niveau entreprise pouvant aller jusqu'à l'ajout ou la suppression d'employés à leur compagnie.

Hormis cet aspect d'administration, il n'existe pas de différentiation des utilisateurs bénéficiaires du service communication suite à leur authentification autre que leur rattachement a une compagnie et l'affectation d'un profile fonctionnel.

2.4.2 Fonctions métier

Les bénéficiaires du service de collaboration Rainbow peuvent voir restreint leur accès au fonctionnel métier pour refléter une politique interne à leur compagnie ou un niveau fonctionnel associé à l'abonnement Rainbow souscrit pour cet utilisateur.

Afin de refléter la politique interne de l'entreprise bénéficiaire, un administrateur métier peut appliquer un profile aux membres bénéficiaires de cette entreprise ajustant les modalités d'usage des fonctions métier. On distingue parmi ces fonctions métiers :

- La messagerie texte sous forme d'échange de messages instantanés. Ces messages peuvent aussi être enrichis de Gifs en provenance de serveurs externes. Cette messagerie peut être

en point à point entre deux bénéficiaires ou en multipoints incluant plusieurs bénéficiaires. Les échanges instantanés sont stockés sur le serveur Rainbow pour permettre de présenter un historique aux bénéficiaires.

- La fonction Bulle est la version multipoint de la messagerie permettant d'inclure plus de 2 bénéficiaires. Cette fonction bulle crée le rôle d'organisateur automatiquement alloué au bénéficiaire créant cette bulle, lui seul hérite des droits de gestion sur le cycle de vie de la bulle : archivage, terminaison.... Celui-ci peut par la suite élever tout autre participant à ce rôle d'organisateur, leur donnant les droits sur la fonction d'appel en audio ou vidéo, permettant d'établir une telle session multipoint entre les participants de la bulle.
- La fonction Partage de fichier met à disposition un espace de stockage de fichier sur le serveur Rainbow dans un but principal de partage.
- La fonction d'appel audio/vidéo permet d'établir des communication audio/vidéo point a point ou multipoint dans le cadre d'une bulle.
- La fonction d'enregistrement permet d'enregistrer un appel audio et historiser celui-ci dans l'espace de stockage du bénéficiaire.
- La fonction de présence publie un état dit de présence liée à l'activité du bénéficiaire. Cette publication s'adresse aux autres bénéficiaires appartenant au réseau de contacts du bénéficiaire publiant. Cet état de présence peut être géré automatiquement par le service Rainbow ou personnalisé par le bénéficiaire s'il en a le droit.

Les autorisations/restrictions d'utilisation de ces fonctions métiers applicables par un administrateur métier aux bénéficiaires sont résumées dans le tableau suivant :

Messagerie	
	Editer et envoyer des messages
	Utiliser des Gifs animés
Bulle (service d'echange multi-utilisateur)	
	Créer et accéder au service
Appel	
	Utiliser des appels Voix sur IP
	Utiliser la vidéo sur IP
Partage de fichier	
	Accéder au service en lecture
	Partager des fichiers
Enregistrement	
	Enregistrer ses conversations
Profil	
	Modifier ses informations personelles
	Modifier ses parametres préféretiels
Présence	
	Modifier son information de présence

La fonction métier bulle, au-delà du créateur de la bulle qui en contrôle le cycle de vie de cette bulle, crée la notion d'organisateur qui est un participant privilégié, ainsi que la notion d'invité. L'initiateur de la bulle se voit attribuer un rôle d'organisateur, qu'il peut transmettre à d'autres participants. Parmi les privilèges associés au statut d'organisateur, on trouve :

- L'ajout et suppression de participants
- La gestion d'un lien URL permettant d'inviter de nouveau participants y compris non bénéficiaires que l'on appelle des 'invités'.
- Promouvoir un autre participant au statut d'organisateur

- Archiver ou supprimer une bulle et son historique de conversation

De plus un organisateur peut contrôler une conférence audio/vidéo avec les membres de la bulle. Son statut d'organisateur lui permet :

- Démarrer ou terminer une conférence
- Contrôler qui rejoint la conférence
- Valider ou couper la source audio d'un participant
- Déconnecter un participant
- Verrouiller la conférence, interdisant ainsi tout nouveau participant de la rejoindre

Le lien URL utilisé par un organisateur pour permettre d'accéder à une bulle peut être révoqué à tout moment par l'un des organisateurs, bloquant tout accès à la bulle. Ce lien est généré par un algorithme le rendant complexe et aléatoire. Un processus de protection contre une tentative de découverte de lien en force brute est mis en œuvre au niveau de l'infrastructure.

2.4.3 Environnement physique

Les ordinateurs et téléphones mobiles sur lesquels sont déployés l'application client Rainbow doivent respecter les prérequis en termes de systèmes d'exploitation et browser supportés. Ils doivent être intègres et mis à jour avec les correctifs de sécurité disponibles auprès des éditeurs de ces systèmes.

Leur accès doit être protégé de façon à renforcer le contrôle d'accès à l'application Rainbow. Pour forcer l'authentification lors de l'établissement d'une session par l'application Rainbow, celle-ci doit être déconnectée par l'utilisateur lorsqu'il ne l'utilise plus.

Seule l'organisation Opération d'ALE (SRE) a accès au déploiement, l'administration système et à la maintenance des composants serveur du service Rainbow. Tout autre acteur ne peut qu'utiliser la partie fonctionnelle du service et sa configuration après avoir été authentifié et uniquement au travers d'une application client Rainbow intègre.

2.4.4 Environnement réseau

L'ensemble des flux est à l'initiative des applications client Rainbow et ne nécessite pas d'ouverture de ports sur l'élément d'accès internet de l'entreprise pour autoriser des flux entrants depuis internet.

Les flux, dit de signalisation, issus d'ordinateurs ou de téléphones mobiles sur lesquels sont déployés l'application client Rainbow sont transportés par les protocoles sécurisés HTTPS/REST (443) et Secure Web Sockets (WSS,443).

Les flux transportant du média vidéo, audio ou partage d'écran sont transportés en utilisant la technologie WebRTC incluant DTLS/SRTP pour la sécurisation. ICE et TURN sont utilisés pour assurer la connexion au travers des éléments d'accès internet et leur protection par NAT/firewall.

A noter que si l'entreprise met en œuvre un proxy HTTP, il doit supporter le protocole Secure Web Sockets.

Les flux sécurisés HTTPS sont réceptionnés cote infrastructure serveur Rainbow par des équilibreurs de charge terminant leur transport crypté.

2.5 Description des dépendances

Au-delà des prérequis sur les systèmes d'exploitation, il faut noter que le déploiement sur le système Microsoft Windows nécessite aussi la présence du package redistribuable Microsoft Visual C++ 2015 x86.

2.6 Définition du périmètre de l’évaluation

L’évaluation porte sur la confidentialité des informations échangées lors de communications établies avec Rainbow. Plus précisément sur le chiffrement des flux entre les clients Rainbow et le service hébergé Rainbow et le chiffrement des flux entre deux clients Rainbow dans le cas de communication point à point. Ces échanges incluent les messages instantanés, les fichiers, les conversations voix et vidéo ainsi que les partages d’écran en point à point ou en multipoint. L’évaluation porte également sur la protection des mots de passe des utilisateurs ainsi que le stockage de fichier sur le serveur.

Le périmètre de l’évaluation de ces fonctionnalités englobe le serveur et les clients exécutés sur navigateur web.

L’évaluation englobe enfin les outils (scripts d’installation) et la documentation utilisés lors de l’installation du produit.

3 Description de l'environnement technique de fonctionnement du produit

La répartition des rôles entre les différents acteurs concernés par la solution Alcatel-Lucent Rainbow est la suivante :

- **Intégrateur** : la solution est entièrement développée et intégrée par **Alcatel-Lucent Enterprise (ALE)**.
- **Bénéficiaires** : ce sont **les utilisateurs finaux** typiquement les employés d'une société ou autres utilisateurs individuels ou invités., Dans le cas d'une société, un employé peut aussi être administrateur métier du service.
- **Fournisseur de socle** : ALE a recours à un fournisseur de socle technique de type *Infrastructure as a Service* (IaaS). En France, **ce fournisseur est la société OVH**
- **Prestataires** : Pour commercialiser et supporter la solution, ALE a recours à un réseau de distribution constitués de **partenaires formés et contractualisés**. Ceux-ci ont accès à une section spécifique du client Rainbow ouvrant des fonctions d'administration métier du service. Ils n'ont pas à gérer le déploiement du logiciel de la partie cloud. Ils peuvent assister les bénéficiaires au déploiement des applications clients Rainbow sur les machines des bénéficiaires.

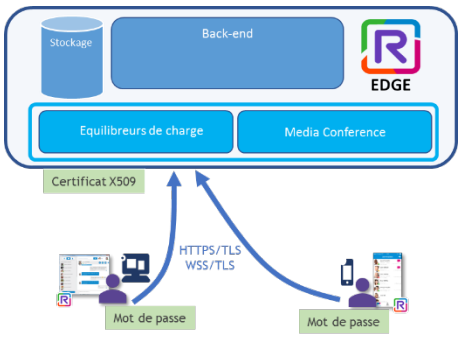
La répartition des rôles entre acteurs se fait selon le tableau suivant :

Utilisateur final	Bénéficiaire		
Administration Métier *Paramétrage*	Bénéficiaire	Prestataire	ALE
Administration Système et Sécurité *Logiciel + OS+ ressources virtualisées*			ALE
Administration de l'infrastructure technique *Couche de virtualisation+machines+Stockage*			OVH
Officier de sécurité *Sécurité des locaux et du personnel*			OVH

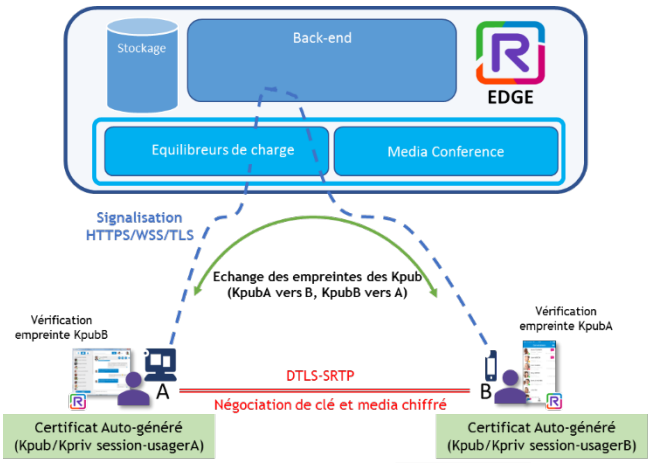
4 Description des biens sensibles

Dans le cadre de cette évaluation, les biens sensibles à protéger sont de diverses catégories :

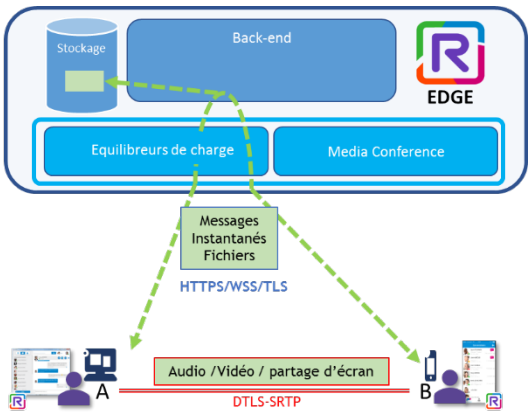
- Les clefs de chiffrement utilisées pour protéger les flux de données
- Les données échangées entre utilisateurs
- Les données stockées
- Les mots de passe utilisateur et administrateur métier



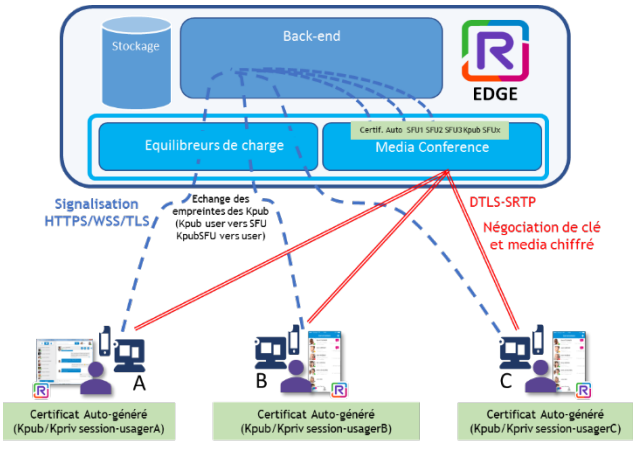
Etablissement de session



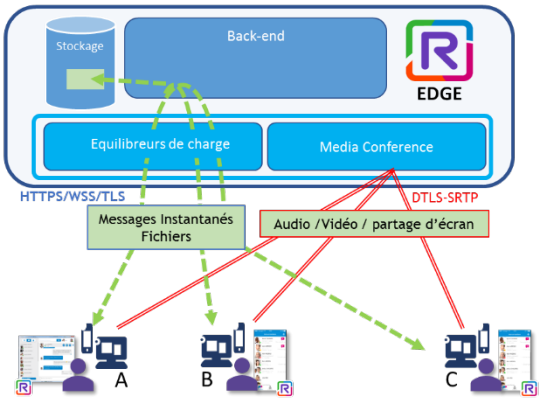
Communication point-à-point – Clefs de session



Communication point-à-point – Flux de données



Communication multi-point – Clefs de session



Communication multi-point – flux de données

On répertorie ces biens et leurs caractéristiques dans le tableau suivant :

Id	Description	Intégrité	Authenticité	Confidentialité
Biens utilisateurs				
B.BiClef.TX	Bi-clef générée et utilisée pour une session de communication			Oui
B.Flux.MSG	Flux de messages instantanés échangés entre utilisateurs	Oui		Oui
B.Flux.Audio	Flux audio échangés entre utilisateurs	Oui		Oui
B.Flux.Vidéo	Flux vidéo échangés entre utilisateurs	Oui		Oui
B.Flux.Ecran	Flux d'écran partagé échangés entre utilisateurs	Oui		Oui
B.Fichier	Fichiers stockés	Oui		Oui
B.MdP.Util	Mot de passe d'ouverture de session			Oui
Biens Administrateur métier				
B.MdP.Admin	Mot de passe d'ouverture de session			Oui
Biens TOE				
B.BiClef.Conf	Bi-clef utilisée par le serveur pour une session multi-point			Oui
B.Certif.serveur	Certificats utilisés par le serveur dans les sessions HTTPS	Oui	Oui	
B.Clef.stock	Clef utilisée par le serveur pour le chiffrement du stockage	Oui		Oui

5 Mesures d'environnement

Hypothèses

Les fonctions d'officier de sécurité, d'administrateur de l'infrastructure technique et d'administrateur système exclusivement assurées par ALE et son fournisseur de socle OVH sont considérées de confiance et non hostiles.

Les utilisateurs finaux et les administrateurs métiers doivent appliquer les consignes de sécurisation de l'accès aux services en utilisant du matériel sain et au logiciel d'exploitation mis à jour régulièrement avec les patches de sécurité disponibles ainsi qu'en gérant leur mot de passe d'accès au service Rainbow de façon sécurisée. Les administrateurs métiers sont considérés de confiance.

Concernant les éléments téléchargés sous forme de fichiers par les bénéficiaires localement sur un ordinateur ou un téléphone mobile depuis le contenu d'un communication Rainbow, il en est de la responsabilité du bénéficiaire de le détruire ou de le stocker de façon sécurisée au-delà de la session de communication afin de le soustraire à un éventuel attaquant prenant le contrôle de son appareil.

L'équipe opération d'ALE assure de son côté l'intégrité des composants logiciels déployés dans le cloud. Elle s'assure de gérer les certificats serveur conformément aux recommandations de l'ANSSI (RGS) et effectue des audits pour détecter les attaques potentielles sur les accès au service. Elle effectue aussi un audit des administrateurs déchus de leurs privilèges par exemple après avoir quitté une entreprise prestataire. Concernant l'aspect stockage, elle sécurise la gestion des clefs utilisées pour le cryptage des données stockées.

Rôles de confiance	
H.RConf.Officier	L'officier de sécurité est considéré de confiance, non hostile et formé au standard de sécurité
H.RConf.Admin.Tech	L'administrateur de l'infrastructure technique est considéré de confiance, non hostile et formé au standard de sécurité
H.RConf.Admin.Sys	L'administrateur du système est considéré de confiance, non hostile et formé au standard de sécurité
Taches de l'utilisateur final	
H.Util.Mdp	L'utilisateur bénéficiaire gère son mot de passe de façon sécurisée et le renouvelle régulièrement. Il lui est demandé de le modifier lors sa première utilisation.
H.Util.Term	L'utilisateur est responsable de la mise à jour du système d'exploitation de son terminal mobile, PC ou MAC supportant l'exécution du client Rainbow. En particulier les patchs de sécurité doivent être régulièrement appliqués.
Taches des administrateurs métier	
H.Admin.Mdp	Les différents administrateurs métier (bénéficiaire, mandataire ou ALE) doivent gérer leur mot de passe de façon sécurisée et le renouvellent régulièrement. Il lui est demandé de le modifier lors sa première utilisation.
H.Admin.Term	Les différents administrateurs métier (bénéficiaire, mandataire ou ALE) sont responsables de la mise à jour du système d'exploitation de leurs terminaux mobile, PC ou MAC supportant l'exécution du client Rainbow. En particulier les patchs de sécurité doivent être régulièrement appliqués.
Taches de l'administrateur système	
H.AdminSys.Vulnérabilité	L'équipe opérations ALE s'assure de la sécurité des différents composants de la solution et de leur mise à niveau le cas échéant pour garantir la sécurité de l'intégralité de l'infrastructure
H.AdminSys.AccesPrivilegié	L'équipe opérations ALE fait une revue régulière des comptes avec privilèges pour vérifier qu'aucun utilisateur déchu de ses privilèges ne puisse continuer a les utiliser.
H.AdminSys.AuditAcces	L'équipe opérations ALE effectue régulièrement des audits internes des différents accès sur l'infrastructure pour détecter toute anomalie suspecte quant à une possible intrusion sur celle-ci
H.AdminSys.Certificat	L'équipe opérations ALE génère et gère les certificats conformément aux recommandations de l'ANSSI (RGS)
H.AdminSys.Stock	L'équipe opérations ALE s'assure de la mise en œuvre du chiffrement du stockage de fichiers échangés par les bénéficiaires et gère les clefs de cryptographie qui y sont associées.

6 Description des menaces

Dans le cadre de l'évaluation, les menaces sur les biens des utilisateur finaux définis précédemment peuvent être portées par des attaquants externes hors bénéficiaires et/ou des attaquants intra-bénéficiaire au sein d'un même entité d'utilisateurs finaux (souvent appelé *Compagnie* dans Rainbow) voire Inter-bénéficiaire, la solution Rainbow implémentant une architecture multi-tenant.

Concernant les flux de données échangées entre bénéficiaires, quelques soit leur type (message instantané, audio, vidéo, partage d'écran), ceux-ci peuvent subir des menaces en aussi bien hors-bénéficiaires, intra ou inter-bénéficiaires. Lors des communications multi-points entre bénéficiaires, il existe un risque de menace d'intrusion par un tiers.

L'authentification des utilisateurs finaux et le contrôle d'accès leur affectant un rôle avec plus ou moins de privilèges peuvent être menacés dans un but d'usurpation et/ou de gain illicite de droits. De même cette menace d'usurpation d'identité et/ou de droit existe aussi pour les administrateurs métiers.

Concernant les biens propres de la TOE, il existe une menace sur les certificats permettant de sécuriser l'établissement des sessions client/serveur HTTPS. Les clefs utilisées pour le stockage sécurisé de fichiers peuvent être menacées.

Menaces hors-bénéficiaires	
M.Données.alteration	Un attaquant tente de modifier des données échangées de tout type (Audio, Vidéo, messages instantanés ou fichiers)
M.Données.Compromission	Un attaquant tente d'intercepter des données échangées de tout type (Audio, Vidéo, messages instantanés ou fichiers)
M.Identité.Usurpation	Un attaquant tente d'usurper l'identité d'un bénéficiaire pour accéder à la solution.
M.Conversation.Intrusion	Un attaquant tente de s'introduire dans une communication multi-points
M.serveur.redirection	Un attaquant tente d'altérer le certificat serveur afin de détourner les sessions HTTPS.
M.Compromission.2Clefclient	Un attaquant cherche a compromettre les flux issus d'un clients
M.Compromission.2Clefclient.Srv	Un attaquant cherche a compromettre les flux issus du serveur lors d'une communication multi-points.
M.Modification.ClefDisk	Un attaquant cherche modifier la clef de chiffrement du stockage de fichier pour accéder ou détruire les données.
M.Compromission.ClefDisk	Un attaquant cherche acquérir la clef de chiffrement du stockage de fichier pour accéder aux données.
Menace Intra-bénéficiaires	
M.Role.Usurpation	Un attaquant tente d'usurper l'identité d'un administrateur métier pour augmenter ses privilèges.

7 Description des fonctions de sécurité du produit

Fonctions de sécurité	
FS.Authentification.usager	Les utilisateurs finaux ou administrateurs métier doivent s'authentifier avant tout accès au service Rainbow lors du démarrage de leur logiciel client. Rainbow utilise de l'authentification basée sur un login mot de passe. Le login est une adresse mèl vérifiée lors de la création du compte par un code à 6 chiffres. Le mot de passe doit être composé d'au moins 12 caractères, avec, une minuscule, une majuscule, un chiffre et un caractère spécial. L'administrateur de l'entité bénéficiaire peut à tout moment réinitialiser le mot de passe d'un bénéficiaire de cette entité. Si le niveau de sécurité n'est pas suffisant, Rainbow permet de s'appuyer sur un service d'authentification externe permettant de mettre en œuvre l'authentification à 2 facteurs, ou des règles de gestion de mot de passe plus strictes. Ce service d'authentification externe ne fait pas partie de l'évaluation.
FS.ControleAcces.usager	Les utilisateurs authentifiés se voient attribués un niveau de service en rapport avec le rôle qui leur est attribué dans leur organisation. Différent rôles sont disponibles afin de gérer le droit d'accès des bénéficiaires. Un bénéficiaire peut être : • Utilisateur du service • Administrateur : permet de gérer les utilisateurs de l'entité bénéficiaire ainsi que les licences associées à chaque bénéficiaire de cette entité. Certains administrateurs ont leur rôle renforcé avec des fonctions d'Opération ou de Finance. Ces rôles n'ajoutent pas de fonctions liées à la sécurité mais purement des fonctions de gestion d'usagers et d'opérations commerciales et donc ne nécessitent pas une évaluation.
FS.Rattachement.Usager	Les utilisateurs authentifiés se voient rattachés à une entité bénéficiaire communément appelée compagnie Rainbow qui assurera le cloisonnement inter-bénéficiaires. Ce rattachement est un rattachement logique qui donne à ce bénéficiaire un moyen de profiter des services disponibles dans cette entité. Ce rattachement peut se faire de différentes façons : • Lors de la création du compte du bénéficiaire directement par un administrateur de l'entité. • L'administrateur de l'entité peut envoyer un email d'invitation que l'utilisateur doit accepter. • Par demande directe de l'utilisateur vers l'entité. Un administrateur de cette entité doit explicitement accepter cette demande.
FS.Protection.Session	Les échanges liés à la session établie entre le client Rainbow et le serveur ainsi que les messages instantanés sont protégés par l'utilisation de HTTPS et d'un tunnel type Web Sockets Sécurisé WSS. Lorsque le bénéficiaire se connecte au service grâce à FS.Authentification.usager, il possède un jeton de session valable 2 semaines, renouvelable 7 fois. Pendant ce laps de temps, le bénéficiaire a accès au service que son niveau d'accès ainsi que ses licences lui donnent droit. Pour être notifié de la réception de nouveaux messages instantanée, et pour que les différentes applications du bénéficiaire restent synchronisées, l'application établie une session XMPP dans une Web socket sécurisée. L'établissement de ce canal de notification est sécurisé par un jeton reçu lors de la connexion au service. Si le bénéficiaire termine son compte ou change de mot de passe, ce canal de notification est fermé automatiquement.
FS.Protection.flux.PaP	Les flux de données échangées (Audio, Vidéo, écran partagés) en point a point entre deux utilisateurs finaux sont sécurisés par l'utilisation de la pile de protocole WebRTC mettant en œuvre DTLS/SRTP. Lorsqu'un bénéficiaire veut établir un appel multimédia avec un autre bénéficiaire, il établit une session basée sur un échange XMPP basée sur la XEP-0166 Jingle. Cela permet de trouver une route afin d'établir le media à travers les différents réseaux disponibles basée sur la technologie WebRTC. Cet échange permet aussi de partager les empreintes des certificats qui seront utilisés pour établir le canal DTLS 1.2. Ce dernier, établi de bout en bout directement entre les bénéficiaires, permet d'échanger les clés à utiliser pour le chiffrement (AES 128) du media via le protocole SRTP. Si le réseau informatique des bénéficiaires mis en relation ne permet pas un routage direct, le flux media peut être acheminé par un serveur intermédiaire (un serveur TURN). Ce serveur intermédiaire ne fait que du routage et n'est pas en mesure de déchiffrer le media et ne remet pas en cause l'aspect chiffrement bout en bout de la communication.
FS.Protection.flux.Multi-points	Les flux de données échangées (Audio, Video, écran partagés) en multi-points entre les utilisateurs finaux sont sécurisés par l'utilisation de la pile de protocole WebRTC mettant en œuvre DTLS/SRTP en incluant une N+1 terminaison au niveau du serveur. L'établissement de la session est identique à celui décrit dans FS.Protection.flux.PaP, excepté que le chiffrement est effectué entre le bénéficiaire et le service de mixage

	afin de pouvoir mixer les flux audio et de les retourner vers les autres bénéficiaires participants. La vidéo et le partage d'écran suivent le même schéma excepté qu'aucun mixage n'est effectué, mais uniquement une transmission vers les autres participants bénéficiaires.
FS.Chiffrement.stockage	Les données des utilisateurs finaux conservés dans le stockage serveur sont chiffrées au repos. Il existe deux catégories de données qui sont stockés de façon chiffré mais différemment. L'historique des messages instantanés, ainsi que les données du profil du bénéficiaire sont stockés en base de données (Maria DB et Mongo DB) sur un system de fichier de type ZFS chiffré au repos. Les fichiers téléchargés et conservé par Rainbow sont dans un system de fichier de type SWIFT chiffré.
Au reposFS.chiffement.MdP	Les mots de passe utilisateurs sont stockes chiffrés et salés dans une base donnée serveur. Le mot de passe fait partie des donnée concerné par FS.Chiffrement.stockage et sont donc conservés de façon chiffré par le system de fichier.

Biens / Menaces	B.BiClef.TX	B.Flux.MSG	B.Flux.Audio	B.Flux.Vidéo	B.Flux.Ecran	B.Fichier	B.MdP.Util	B.MdP.Admin	B.BiClef.Conf	B.Certif.serveur	B.Clef.stock
M.Données.alteration		x	x	x	x						
M.Données.Compromission		x	x	x	x						
M.Identité.Usurpation								x			
M.Conversation.Intrusion		x	x	x	x						
M.serveur.redirection							x			x	
M.Compromission.2Clefclient	x										
M.Compromission.2Clefclient.srv									x		
M.Modification.ClefDisk						x					x
M.Compromission.ClefDisk						x					x
M.Role.Usurpation								x			

	M.Données.alteration	M.Données.Compromission	M.Identité.Usurpation	M.Conversation.Intrusion	M.serveur.redirection	M.Compromission.2Clefclient	M.Compromission.2Clefclient.srv	M.Modification.ClefDisk	M.Compromission.ClefDisk	M.Role.Usurpation
Hypothèses										
H.RConf.Officier					x			x	x	
H.RConf.Admin.Tech					x			x	x	
H.RConf.Admin.Sys					x			x	x	
H.Util.Mdp	x	x	x							
H.Util.Term	x	x	x							
H.Admin.Mdp	x	x	x							x
H.Admin.Term	x	x	x							x
H.AdminSys.Vulnérabilité	x	x	x	x	x	x	x	x	x	x
H.AdminSys.AccesPrivilegié	x	x								x
H.AdminSys.AuditAcces	x	x			x			x	x	x
H.AdminSys.Certificat	x	x	x	x	x	x	x	x	x	x
H.AdminSys.Stock								x	x	
Fonctions de sécurité										
FS.Authentification.usager			x	x	x				x	x
FS.ControleAcces.usager			x	x	x				x	x
FS.Rattachement.Usager			x	x						x
FS.Protection.Session	x	x				x	x			
FS.Protection.flux.PaP	x	x				x				
ES.Protection.flux.Multi-points	x	x					x			
FS.Chiffrement.stockage	x	x						x		
FS.chiffement.MdP			x							x

End of Document