Jour 2 : serveur de communication, fonctionnalités

Objectifs du jour 2

- 1.1 Connaît les différentes possibilités de solutions des serveurs de communication (par ex. sur site, cloud, virtuel).
- 1.2 Connaît les exigences importantes posées aux appareils de communication (par ex. sécurité, profil de charge, volume de données, segmentations, qualité de service, disponibilité des services nécessaires, interfaces, dispositifs terminaux).
- 1.3 Connaît les formes de présentation afin de consigner les exigences par écrit.
- 4.1 Connaît les fonctions importantes d'un serveur de communication (par ex. conférence téléphonique, ligne directe, mise en attente, réception de messages vocaux et de télécopies par e-mail, transmission, musique d'attente, liste noire).
- 4.2 Connaît les variantes de connexion pour synchroniser les utilisateurs et les attributs de systèmes tiers (par ex. Active Directory).
- 4.3 Connaît les méthodes pour gérer et administrer les téléphones de manière centralisée.

Les différentes possibilités de solutions des serveurs de communication (1.1)

Cette thématique a déjà été dégrossie dans le support de cours du premier jour. Nous allons donc résumer en quelques points les différentes solutions possibles.

Pour commencer, parlons du lieu où sera installé le système de téléphonie. Nous pouvons en identifier 2, soit :

- Sur le site principal (physique) ou sur l'infrastructure du client final, ce que l'on nomme également une solution On Premise. L'infrastructure appartient en général au client final est c'est à lui ou à un autre prestataire de la maintenir.
- Sur un Cloud privé ou publique, dans un Datacenter avec une infrastructure fournie par le client lui-même ou louée à un prestataire, voire directement hébergé chez un opérateur ou fournisseur de la solution de téléphonie. Dans la majeure partie des cas, l'infrastructure n'appartient pas au client final et est maintenue dans le cadre de la location par l'opérateur ou le fournisseur de services.

Ensuite, parlons du type d'installation du système de téléphonie. Nous pouvons en identifier 3 soit :

- Avec une appliance physique. Ce type d'installation est plus souvent réalisé directement chez le client final (On Premise). La nécessité d'un matériel physique peut être dû à plusieurs facteurs, notamment la possibilité d'ajout de cartes spécifiques (carte d'extensions analogiques ou numériques propriétaire, carte avec module relais, …). Certains clients ne veulent pas de solution hébergée dans le Cloud et préfèrent disposer de tous leurs équipements à proximité, dans leurs locaux. Ce type d'installation nécessite une connectivité à Internet fiable, notamment pour l'interaction avec le fournisseur de téléphonie ou opérateur. Une panne de l'accès à Internet a donc un très fort impact sur le fonctionnement de cette solution.
- Avec une appliance virtuelle. Ce type d'installation peut être réalisé tant chez le client (On Premise) ou sur une infrastructure Cloud. Une infrastructure fiable doit être disponible chez le client afin de pouvoir héberger le système de téléphonie virtuel. La connectivité (expliquée au point précédent) est également très importante. Les contraintes d'un hébergement local sont donc plus importantes. Pour une installation sur une infrastructure Cloud, les contraintes de disponibilités sont toujours prises en compte et l'environnement dispose, en règle générale, de dispositifs de sécurité accrus (redondance d'accès Internet, redondance d'alimentations électriques, redondance de hardware, …). Cette solution permet également de gérer plus facilement des sites distants, notamment si le client possède plusieurs succursales.
- Avec une solution hybride. Ce type d'installation est un mix des deux solutions précédentes et utilise des appliances physiques et virtuelles simultanément. Cette implémentation permet, par exemple, une certaine redondance et une autonomie de chaque site pouvant travailler de manière indépendante tout en étant interconnectés.

Une remarque, déjà abordée mais extrêmement importante pour l'installation de ces différentes solutions, est la fiabilité de l'infrastructure réseau et de la connectivité à Internet. Une redondance devrait être envisagée dans chaque projet, en fonction des besoins du client.

Mandat 1 : recherche quelles sont les différentes possibilités d'installation de ton système de téléphonie (On Premise, Cloud, machine physique, machine virtuelle…). Liste les avantages et les contraintes en fonction des différentes possibilités.

Les exigences importantes posées aux appareils de communication (1.2)

Actuellement, avec l'avancée importante de la ToIP, les terminaux IP sont soumis à de fortes contraintes au niveau de la sécurité et de la fiabilité dans la conception de l'appareil. Le mise en place de la ToIP constitue de nouvelles opportunités d'attaques dans le monde des systèmes d'informations. La signalisation et la voix partageant le même réseau ou au moins les mêmes technologies que les réseaux de données IP, la téléphonie partage les mêmes vulnérabilités que les réseaux de données. A cela il faut rajouter les risques propres à la signalisation de la ToIP et au transport de la voix.

Voici une liste non-exhaustive des risques liés à la ToIP :

- Déni de service DoS
- Ecoute clandestine
- Détournement de trafic
- Usurpation d'identité
- Vols de services
- Communications indésirées SPIT (Spam over Internet Telephony)

L'autre manière de définir la menace est de caractériser les attaques. Ces dernières permettent à un élément menaçant d'exploiter une vulnérabilité. Les attaques de la ToIP peuvent se ranger en trois grandes familles explicitées dans le tableau ci-dessous :

Type d'attaque	Principe du mode opératoire
Interception et modification	- Collecte d'informations sur les communications - Collecte d'informations sur les utilisateurs et le réseau - Manipulation du contenu des communications - Détournement des communications - Écoute des communications (conversation, message, vidéo)
Fraude et abus de service	- Usurpation d'identité - Contournement, porte dérobée (back door) - Manipulation des données de facturation
Interruption de service ou déni de service (DoS)	- Coupure physique - Épuisement des ressources - Déni de service général

Quelles sont donc les propriétés importantes en matière de sécurité ? Voici une liste de 6 points primordiaux :

- **L'authentification** : garantir l'identité de l'usager qui envoie le message
    - dans le cadre de la ToIP, cette propriété permet par exemple à un serveur de vérifier qu'il fournit le service à l'usager légitime
- **La confidentialité** : rendre la conversation compréhensible aux personnes concernées uniquement
    - dans le cadre de la ToIP, cette propriété nécessite de chiffrer le flux audio
- **L'intégrité** : s'assurer que les données n'ont pas été modifiées entre l'envoi d'un message et sa réception
    - dans le cadre de la ToIP, cette propriété permet de s'assurer que les paramètres d'un appel n'ont pas été modifiés par une tierce partie
- **La non répudiation de l'appel** : la non répudiation des données nécessite l'archivage des données échangées
    - dans le cadre de la ToIP, cette propriété permet d'associer une communication à une personne de manière certaine
- **Le non rejeu** : éviter de mémoriser puis de réinjecter les données dans le réseau
    - dans le cadre de la ToIP, cette propriété permet de ne pas pouvoir rejouer des échanges protocolaires par une personne tierce souhaitant accéder au service
- **L'anonymat** : capacité du système à masquer l'identité de l'usager
    - dans le cadre de la ToIP, cette propriété peut se traduire par le masquage de l'identité de l'appelant

Les solutions pour sécuriser la ToIP existent. Elles font l'objet de recommandations formalisées par divers acteurs du domaine. Le document édité par le NIST est une référence. Les méthodes de sécurisation usuelles s'appuient donc sur les 5 grands principes suivants :

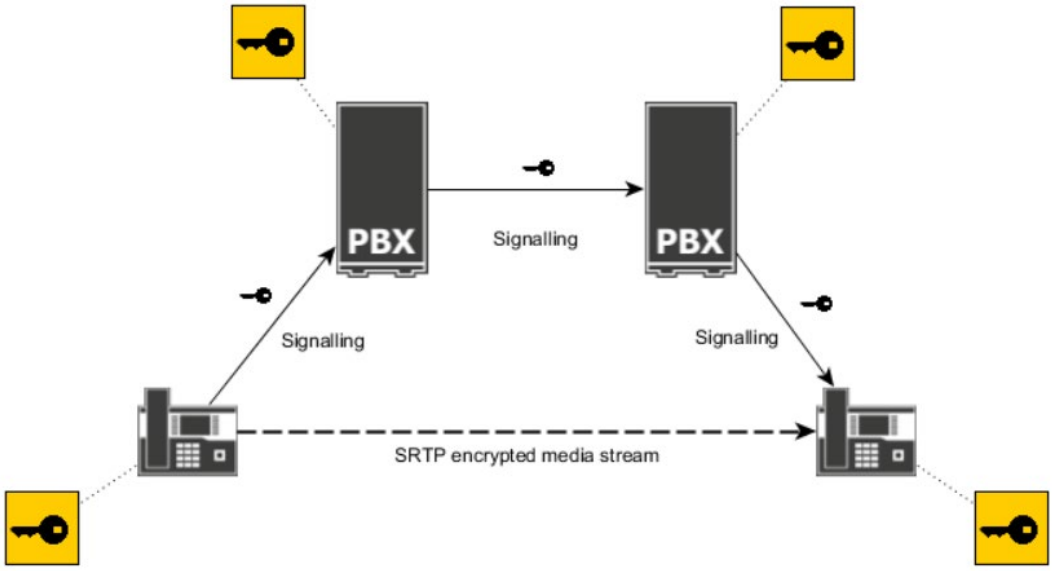
- Les bonnes pratiques
- La séparation des équipements voix/données
- L'authentification
- La confidentialité

- La sécurité périmétrique.

En résumé, il est donc essentiel de protéger et sécurisé les 3 points suivants :

- L'infrastructure logiciel ou physique (serveur, téléphone, …) nécessaire pour recevoir et émettre des appels
- La voix : la conversation téléphonique
- La signalisation : les informations nécessaires à l'établissement de l'appel ou aux services de téléphonie associés au compte usager

Les terminaux doivent donc respecter ces différentes exigences en matière de sécurité. Les protocoles SIPS et SRTP devraient donc y être implémentés. Grâce à SIPS/SRTP, une connexion sécurisée d'égal à égal est utilisée non seulement pour l'audio, mais aussi pendant que la connexion est établie. Cela signifie que le son n'est pas le seul à être crypté, mais aussi les détails de la connexion (qui appelle qui, etc.). Pour utiliser ces protocoles sécurisés, tous les appareils concernés doivent prendre en charge les protocoles SIPS et SRTP. Si l'un des homologues ne prend pas en charge ces protocoles, il n'est pas possible d'établir une connexion sécurisée. Il est recommandé d'utiliser SIPS et SRTP dans les scénarios où l'on peut s'attendre à des attaques du monde extérieur (c'est-à-dire dans le nuage ou si aucun VPN n'est disponible).



Les terminaux SIP ont également une interface de management permettant de réaliser certains paramétrages spécifiques. Cette interface est souvent atteignable au moyen des protocoles WEB HTTP et HTTPS. Actuellement, seul le protocole HTTPS devrait être utilisé pour une raison évidente de sécurité de l'accès.

En plus des exigences de sécurité, il peut également avoir des exigences liées au matériel et à sa conception, notamment pour des terminaux spéciaux comme :

- Les terminaux ATEX (L'objectif du matériel ATEX est de prévenir des explosions en garantissant que les équipements utilisés dans les environnements dangereux sont conçus et construits de manière à minimiser les risques)
- Les terminaux antibactériens : le but du matériau utilisé est d'empêcher le développement et la prolifération des bactéries. Ce genre de terminaux peut être utilisé dans les hôtels ou les hôpitaux.

Les formes de présentation afin de consigner les exigences par écrit (1.3)

Afin de pouvoir discerner au mieux les besoins des clients, il devient nécessaire de réaliser des checklists permettant de spécifier très précisément le matériel devant être proposé en adéquation avec l'infrastructure du client final. Comme nous l'avons vu au point précédent, les contraintes sont multiples, notamment en matière de construction physique des terminaux mais également en matière d'implémentation afin de respecter des règles strictes de sécurité.

En plus de checklists, il devient également très important de réaliser un schéma complet de l'installation, par exemple avec Visio, afin de conceptualiser et visionner rapidement l'infrastructure du client final.

Un document d'inventaire répertoriant avec précision le matériel installé chez le client est également très important. En effet, avec l'évolution du matériel, il est capital de pouvoir proposer rapidement des améliorations et de remplacer le matériel devenu obsolète (EoL, EoS, …). Les versions de firmware doivent notamment y être documentées.

La gestion des mots de passe est également un thème critique. Elle devrait être gérée de façon autonome par l'utilisation de logiciels appropriés (par exemple, Keepass, Keeper, …). En aucun cas, des mots de passes devraient être visibles dans un schéma ou dans une checklist de matériel. L'accès à ce gestionnaire devrait également être sécurisé, notamment par l'utilisation de logins et mots de passes propres à chaque technicien, mais aussi par une solution d'authentification à double-facteur. Les données doivent impérativement être sécurisées et sauvegardées sur différents supports de sauvegardes.

Une dernière étape importante est celle du décommissionnement des anciens appareils comme les appliances physiques, les terminaux, … Aucune information de l'ancien propriétaire du matériel ne devrait être disponible une fois qu'il est démonté et éliminé. Une étape de remise à zéro des appareils doit être impérativement planifiée.

Mandat 2 : établir une checklist reprenant les différents thèmes du point précédent afin de pouvoir fixer précisément les besoins du client final (choix des terminaux, gestion de la sécurité, …). Etablir également un schéma de l'installation et un inventaire du matériel installé (SN, MAC address, version de firmware, …). Utiliser un système de gestion de mots de passes spécifiques afin de les répertorier.

Les fonctions importantes d'un serveur de communication (4.1)

Chaque serveur de communication dispose de plus ou moins de fonctions à la disposition des utilisateurs finaux. Certaines fonctions de base se retrouvent sur tous les systèmes du marché. Par contre, des fonctions étendues peuvent également être fournies ou non. Il est à relever que, concernant les plateformes hébergées directement chez les opérateurs ou fournisseurs, celles-ci disposent, en règle générale, des fonctions de bases. Les fonctions étendues font, par contre, souvent défaut. Il n'est par rare, en fonction des besoins spécifiques des utilisateurs finaux, de devoir migrer d'une plateforme hébergée vers un serveur de communication plus adaptés et permettant une plus grande souplesse dans les configurations, notamment en lien avec des fonctionnalités avancées.

Prenons l'exemple d'un voicemail. Sur une plateforme hébergée, ce service est souvent relativement basique et permet l'enregistrement d'une, voire deux annonces. Certains utilisateurs nécessitant un plus grand nombre d'annonces (comme les médecins par exemple) ne pourront donc pas se satisfaire d'un système hébergé, trop restrictif. Il faudra donc leur proposer un serveur de communication plus adapté, permettant un nombre plus important d'annonces.

Quand nous parlons de fonctionnalités, nous pouvons penser à :

- Gestion des appels, renvois, déviations, …
- Gestion de présence (disponible, absent, ne pas déranger, …)
- Gestion de parking d'appels
- Groupes d'appels
- Système d'auto-attendant avec gestion d'agents et de files d'attentes
- Gestion de la musique d'attente
- Gestion d'annonces et de messages vocaux
- Gestion des utilisateurs, permissions, droits, …
- Gestion de systèmes IVR
- Intégration de système tiers
- Gestion des fax
- Gestion de la connectivité SIP avec l'opérateur, gestion des codecs
- Gestion de système de visio-conférence
- Gestion d'une messagerie ou d'un chat interne
- Gestion et attribution des numéros externes aux utilisateurs
- Gestion de calendrier et de fonctions automatisées
- Gestion de l'enregistrement des appels
- …

Cette liste n'est de loin pas complète.

Les fonctions principales et étendues de 3CX sont résumées sur cette page :
https://www.3cx.com/ordering/pricing/features/

Le système 3CX fourni une tabelle avec tous les services disponibles en fonction du type de licence choisi.

Mandat 3 : recherche les différentes fonctionnalités disponibles sur ton système et fait un comparatif avec un autre système de ton choix, comme, par exemple un système hébergé chez un opérateur ou un fournisseur. Quels sont les avantages et les inconvénients des systèmes proposés ? Quels sont les coûts liés au système choisi ? Quel système te semble être le plus approprié ?

Les variantes de connexion pour la synchronisation des utilisateurs (4.2)

En fonction du système choisi, il est possible d'avoir une intégration avec un certains nombre de systèmes tiers. Diverses fonctionnalités complémentaires s'offrent alors aux utilisateurs et permettent une meilleure intégration aux autres applications de l'entreprise. Voici une liste non-exhaustive de systèmes tiers :

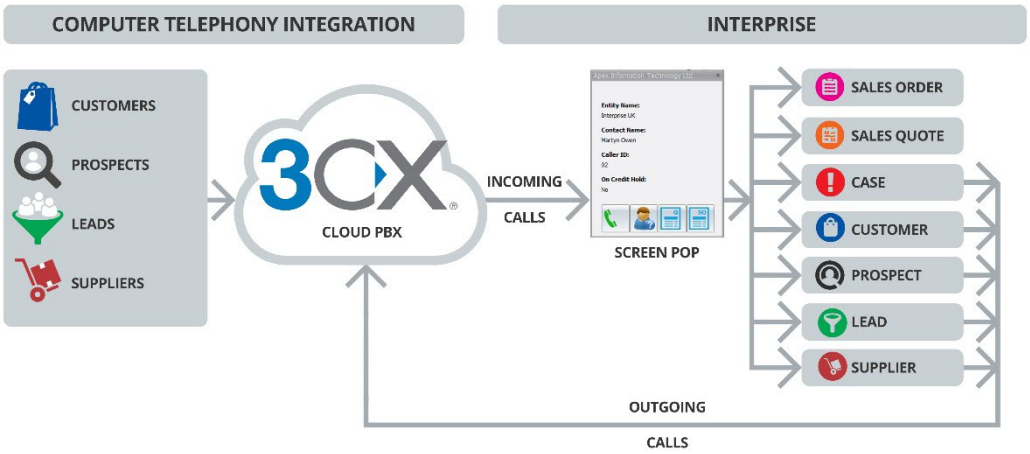
- Gestion des utilisateurs internes (extensions) et intégration de calendriers et de contacts avec Microsoft, Google, …
- Interaction avec des outils de CRM, par exemple, Salesforce, Zendesk, Freshdesk, Bitrix, Odoo, …
- Interaction avec des outils hôteliers comme Fidelio, Mitel, …
- Interaction avec Teams
- Interaction avec des systèmes de messagerie instantanée comme WhatsApp, services SMS, …
- Interaction avec les réseaux sociaux comme Facebook, …
- Interaction avec des systèmes de taxation comme Easytax, …
- Interaction avec des systèmes d'alarmes ou d'appel malade, comme Siemens, Tyco, GETS, …

Il y aura certainement encore d'autres intégrations possibles, certains systèmes étant plus développés et aboutis que d'autres.

Avec la solution de 3CX, les interactions suivantes sont possibles :

- Intégration M365 et Azure AD : https://www.3cx.com/docs/manual/microsoft-365/
- Intégration Google : https://www.3cx.com/docs/manual/google-sso/
- Intégration des contacts : https://www.3cx.com/docs/manual/phonebook/

- Intégration de CRM : https://www.3cx.com/docs/crm-integration-guides/
- Intégration avec Teams : https://www.3cx.com/docs/microsoft-teams/
- Intégration avec WhatsApp : https://www.3cx.com/docs/manual/whatsapp/
- Intégration avec Facebook : https://www.3cx.com/docs/manual/facebook/
- Intégration avec des solutions PMS : https://www.3cx.com/docs/pms-integration/
- Intégration avec des systèmes de taxation : https://www.3cx.com/docs/billing-interface/ avec le formatage des CDR : https://www.3cx.com/docs/cdr-call-data-records/
- Intégration avec des systèmes d'alarmes et de gestion du bâtiment : https://evolink.ch/en/services-en/telecom/nurse-call-system/



Chaque système travaille avec une tabelle de paramètres propres qui permet de définir des réglages et configurations particuliers du système. Certains fournisseurs sont plus généreux que d'autres dans la diffusion de ces paramètres en y donnant pleinement accès. D'autres préfèrent garder leur système propriétaire et développent un serveur permettant de communiquer avec le système et tout équipement ou système tier.

Le système 3CX fournit une tabelle avec tous les paramètres utilisés : https://www.3cx.com/docs/parameters-table/

Mandat 4 : recherche les différentes possibilités d'interaction de ton système avec des systèmes tiers et recherche également les caractéristiques des paramètres de ton système, s'ils sont disponibles. Réalise également une intégration d'un système tiers (Annuaire, CRM, …) avec ton serveur de communication et test le bon fonctionnement de cette intégration.

Gestion et administration des téléphones de manière centralisée (4.3)

La plupart des constructeurs de terminaux proposent un système de management et de provisioning centralisé. Cet outil est souvent appelé un serveur RPS (Redirection and Provisioning Service). Les fonctionnalités offertes varient entre les différents fournisseurs. L'accès au serveur peut être configuré par soi-même en créant un compte et en s'identifiant. Pour d'autres, il faut faire une demande spécifique au fournisseur qui enverra les informations nécessaires à la création d'un compte de gestion.

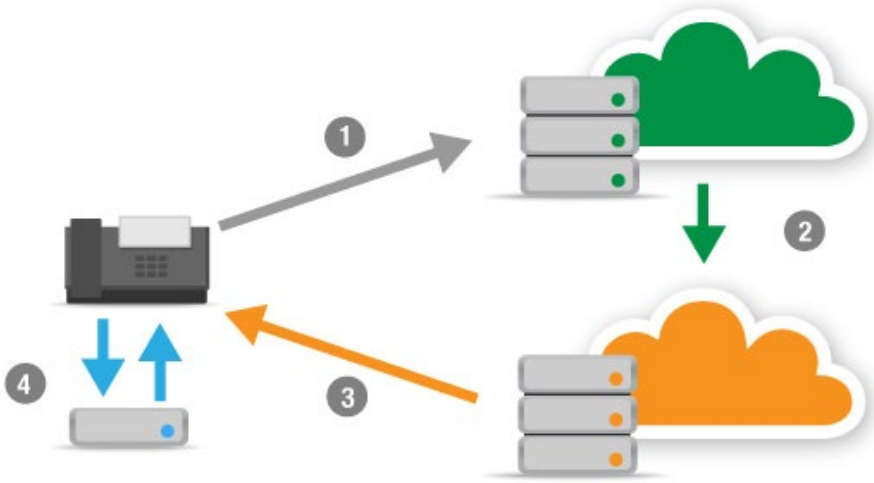
Voici une liste non-exhaustives de fournisseurs proposant un serveur RPS.

- Grandstream : https://www.gdms.cloud/login
- Yealink : https://dm.yealink.com
- Snom : https://sraps.snom.com/
- Fanvil : https://fdps.fanvil.com/

Les fonctionnalités suivantes peuvent être disponibles :

- Gestion basique des terminaux
- Gestion avancée des terminaux
- Possibilités de mise à jour à distance des terminaux
- Possibilités de redémarrage à distance des terminaux
- Indication du système de téléphonie sur lequel un terminal doit être affecté
- Gestion de comptes VoIP
- Journaux d'événements
- Diagnostics
- Connectivité avec des systèmes tiers au moyen d'API's (Application Program Interface)

Le but premier de ces serveurs RPS est d'automatiser et de simplifier un maximum la gestion des terminaux. Il est par exemple possible d'envoyer directement un terminal au client final, lui demander les informations nécessaires (SN, MAC Address, type, …), configurer le serveur RPS et le serveur de téléphonie. Le client final n'a plus qu'à connecter son terminal et la configuration et les mises à jour seront effectuées automatiquement. Ceci permet de limiter le nombre d'interventions sur site et de réduire les coûts pour le client final.



1. On boot-up, the Yealink IP phone attempts to connect to Yealink's master RPS server.

2. The Yealink RPS server receives the request from the phone; if the phone's MAC address is registered on the RPS system, the Yealink server communicates back to the phone that configuration information is available on the VoIPon server.

3. The Yealink phone retrieves the encrypted configuration file from the VoIPon server which is pre-populated at the order stage with extension and server variables.

4. Using the retrieved configuration file, the Yealink phone configures and connects to the PBX or VoIP Provider as instructed.

Mandat 5 : Dans la mesure du possible, crée ou utilise un compte sur un serveur RPS en lien avec les terminaux à ta disposition. Fait le nécessaire afin d'automatiser l'installation d'un terminal sans devoir t'y connecter localement pour le lier avec ton système de téléphonie VoIP. Fais une recherche sur les différentes plateformes RPS proposées.

Sources :

https://evolink.ch/en/services-en/telecom/nurse-call-system/

https://www.3cx.com/docs/

https://www.3cx.com/docs/manual/

https://www.3cx.com/ordering/pricing/features/

https://www.3cx.com/blog/voip-howto/import-active-users-azure/

https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-91576.html

https://www.ictjournal.ch/news/2022-11-18/des-obligations-plus-strictes-pour-les-operateurs-et-fai-suisses

https://www.ringcentral.com/fr/fr/blog/glossaire/protocole-sip/

https://pastel.hal.science/pastel-00559130v1/file/Manuscrit_ThA_se_Thomas_Guillet_version_23_janvier_2011_-_13h45.pdf

https://www.3cx.fr/voip-sip/

https://askozia.com/voip/what-is-sips-and-srtp/

https://fitsmallbusiness.com/voip-security-threats/

https://wiki.innovaphone.com/index.php?title=Reference11r1:Concept_DTLS-SRTP

https://www.voipon.co.uk/pages/rps_benefits.php