# DEFINITION D'UNE ARCHITECTURE DE TELEPHONIE SUR IP SECURISEE

*Ce chapitre porte sur la définition et la spécification d'une architecture pour une sécurité de bout-en-bout de la téléphonie sur IP. Cette architecture se distingue par une mise en œuvre d'une signalisation sur le canal du media. Ceci permet une interopérabilité avec tout type d'infrastructure notamment de signalisation de ToIP. « Future Narrow Band Digital Terminal » et « Secure Voice over IP Simple Protocol » basés sur ce principe seront analysés dans ce chapitre. De cette analyse des exigences sont déduites pour la définition et la spécification d'une architecture « robuste et sécurisé » de ToIP basé sur le canal du media.*

## 6. Définition d'une architecture de téléphonie sur IP sécurisée

### 6.1. Sécuriser les appels de bout-en-bout

La téléphonie sur IP est basée sur une multitude de protocoles. Ces derniers interopèrent globalement entre eux pour la gestion des appels. La continuité concerne principalement les fonctions de base de la signalisation et l'acheminement de la voix. La sécurité est quant à elle propre à chaque infrastructure et ne fait l'objet d'aucune spécification au niveau des interconnexions. La sécurité des appels de bout-en-bout repose donc sur une cohérence des protocoles et des politiques de sécurité mis en œuvre. Cependant avec la multiplication des technologies, des protocoles, des opérateurs, cette configuration n'est pas celle rencontrée.

Pour contourner cette hétérogénéité, deux protocoles Future Narrow Band Digital Terminal [FNBDT] et Secure Voice over IP Simple Protocol [BAS05] ont proposé une solution applicative complètement indépendante de l'infrastructure sous-jacente. Elles établissent une signalisation de sécurité dans le canal média après l'établissement de l'appel. Cette approche permet d'avoir une solution complètement interopérable avec l'environnement de la téléphonie sur IP actuel. Nous avons analysé ces solutions pour vérifier leur robustesse et leur adéquation avec les architectures de ToIP. Notre travail a montré qu'ils restaient encore des points achoppements pour une mise en œuvre généralisée dans un environnement IP. Pour corriger ces vulnérabilités, une architecture de ToIP sécurisée sera ainsi spécifiée.

## 6.2. Sécurité de bout en bout basée sur une infrastructure hétérogène

### 6.2.1. *Future Narrow Band Digital Terminal & Secure Communication Interoperability Protocol*

Future Narrow Band Digital Terminal (FNBDT) et son évolution Secure Communication Interoperability Protocol (SCIP) sont des solutions applicatives de sécurité pour la téléphonie. Ces protocoles proposés par la NSA pour les services gouvernementaux américains ont été depuis adoptés par l'OTAN. Ils sont décrits dans différents documents mais seul le plan de signalisation de FNBDT [FNBDT] est public comme le confirme [GAU09]. L'ensemble des spécifications (gestion des clés, condition d'interopérabilité, le vocodeur et certaines informations cryptographiques) sont réservées aux services étatiques et aux industriels.

FNBDT pose le principe d'une signalisation de sécurité échangée dans le canal média. Il ne spécifie donc pas les modalités d'établissement de l'appel qui sont à la charge de l'infrastructure téléphonique (cf. figure 60) Les échanges de messages permettent donc les services suivants :

- la signalisation de contrôle nécessaire pour initier, maintenir, et terminer les modes sécurisés ;
- la sélection du mode dit « opérationnel » : voix non sécurisée, voix sécurisée, données chiffrées ;
- la synchronisation et les choix cryptographiques.

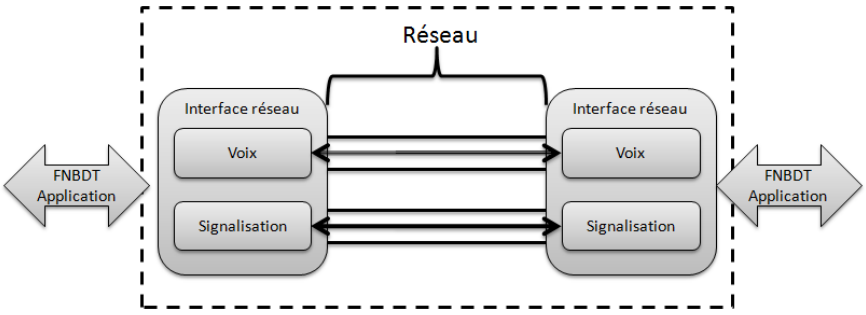


Figure 60. Application FNBDT dans l'infrastructure de téléphonie sur IP

FNBDT s'appuie sur une architecture protocolaire pour mettre en œuvre la signalisation mais également les autres services comme le transport, le chiffrement, le vocodeur. L'organisation des différents modules de l'application (cf. figure 61) est la suivante :

- les modules du haut de la pile est composé de différents applicatifs chargés de l'établissement de l'appel sécurisé, la gestion des clés, le transport des données, le vocodeur MELP[30] [SUP97] ;

[30] MELP : Mixed Excitation Linear Prediction est un vocodeur à 2400 bits/s développé par les services gouvernementaux américains.

- la couche de chiffrement qui chiffre et déchiffre les informations échangées ;
- la couche message ;
- la couche transport qui connait deux modes. Le premier « Mode Framed » permet un transport fiable avec accusé de réception. Le deuxième « Mode Fullbandwidth » qui permet une transmission tolérant des erreurs, des rejets et des pertes d'informations.

Pour garantir le succès des échanges de signalisation et des données de contrôle, FNBDT utilise des mécanismes de fiabilisation. Plusieurs mécanismes sont mis en place comme le Forward Error Control[31] (FEC), le Cyclic Redundancy Check CRC, des acquittements et des règles de rejet [DAN02-1]. Ces mécanismes sont utilisés quelles que soient les propriétés de la couche transport. Bien que conçu pour de nombreux types de liaisons (tactiques, civils, filaires, radioélectriques,...), FNBDT est une solution orientée « commutation de circuit », c'est à dire pour un lien avec des ressources réservées et des caractéristiques constantes. Le passage à l'IP (commutation de paquets) introduit de nouveaux problèmes comme la variation des délais d'acheminement et la perte de paquets.

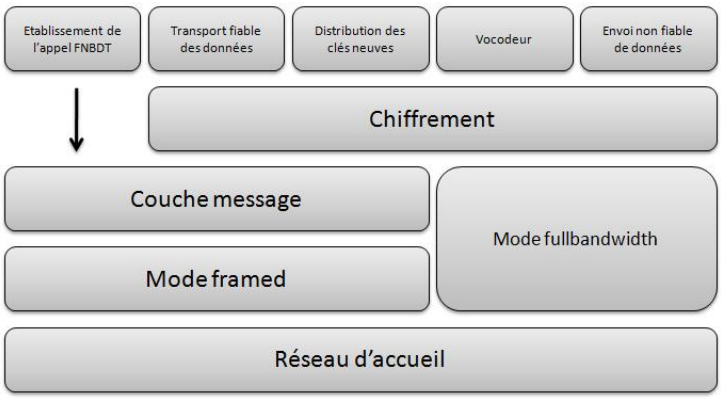


Figure 61. Architecture protocolaire FNBDT

Dès 2001 [DAN01] identifiait certaines limites. En mode trame, la transmission émise par la couche message est encapsulé dans un groupe de 127 trames maximum. En considérant les messages de début SOM (Start of message) et de fin EOM (End Of Message) ainsi que les 125 trames classiques, la super trame atteint 2556 octets. La couche transport du modèle TCP/IP va donc fractionner la transmission en fonction de la taille maximum des trames pouvant être transportée par le réseau (i.e. la taille maximale d'une trame est 1500 octets en *Ethernet*). Ce fractionnement et la gigue vont augmenter le délai de reconstruction de la transmission pouvant générer une augmentation de la surcharge protocolaire. Bien que le principe de la solution applicative semble simple, FNBDT et

[31] FEC et CRC : Forward Error Correction et Cyclic Redundancy Check sont des mécanismes de protection contre les erreurs dues à la transmission de données. L'émetteur ajoute de la redondance afin de permettre au destinataire de détecter et de corriger une partie des erreurs. Cela permet d'éviter la retransmission et d'économiser de la bande passante.

SCIP font l'objet d'études de fonctionnement sur les différents liens comme la HF [ALV07], la VHF/UHF [ALV09] et l'IP/3G [DAN02-2]. Une totale interopérabilité nécessite de nombreuses simulations et validations pour garantir le fonctionnement sur tout type de réseaux.

Nous allons maintenant étudier l'établissement de l'appel sécurisé. Quand un canal média est ouvert entre les deux terminaux FNBDT, le premier message envoyé ou reçu est le message « Capabilities ». Celui-ci contient toutes les informations qui permettent de contrôler, d'évaluer les compatibilités et de décider quels algorithmes utilisés. Au cours de ce premier échange, le mode « opérationnel » est choisi : mode clair ou chiffré, ou transfert de données. C'est à ce moment également que l'on choisit le type de clés (nationale ou OTAN).

Dans la mesure où le mode clair n'est pas retenu, les messages Capabilities sont suivis des messages suivants :

- les « Parameters/Certificate » messages contenant les paramètres associés au mode opérationnel choisi et le certificat de l'usager ;
- les « Foward and Reverse F(R) » messages pour l'établissement de la clé secrète (non défini dans [FNBDT]) ;
- les « Cryptosync » messages pour la synchronisation et le contrôle du mode chiffré.

La chronologie de l'appel est illustrée en figure 62. L'architecture de gestion des certificats et les modalités de distribution ne sont décrites dans [FNBDT].

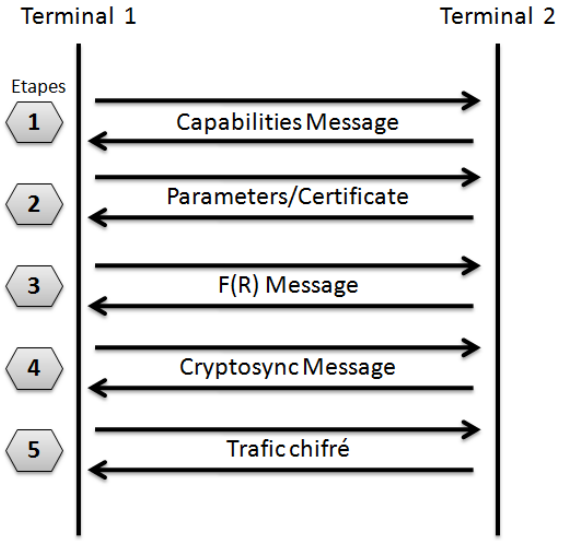


Figure 62. Etablissement d'un appel FNBDT

Cette architecture présente cependant des spécifications qui nous paraissent être des vulnérabilités :

- ce protocole ne prévoit pas d'authentification explicite des usagers avant les messages « Capabilities ».

- la signalisation est en claire ce qui permet à un attaquant en coupure de forcer le mode clair. Si la vérification des certificats n'est pas réalisée, le pirate peut également les modifier.
- il n'y a pas de mécanisme d'intégrité ;
- le protocole a été développé pour les réseaux à commutation de circuit. La couche transport doit être adaptée aux réseaux IP.

### 6.2.2. *Secure Voice over IP Simple Protocol*

Secure Voice over IP Simple Protocol (SVSP) défini par Carole Bassil [BAS05] est une solution qui a été conçu nativement pour la ToIP. L'appel sécurisé est également séparé en deux parties : la signalisation pour sécuriser l'appel et l'appel sécurisée proprement dit. Cette solution s'appuie cependant de manière explicite sur des éléments de confiance qui sont :

- **une carte à puce** stockant les éléments de sécurité nécessaire au fonctionnement de l'application ;
- l'entité de confiance distribuée appelée **« Trusted Authentication Autority » (TAA)** ;
- l'entité de confiance racine appelée **« Global Truster Authentication Autority » (GTAA)**.

L'architecture matérielle est illustrée par la figure 63.

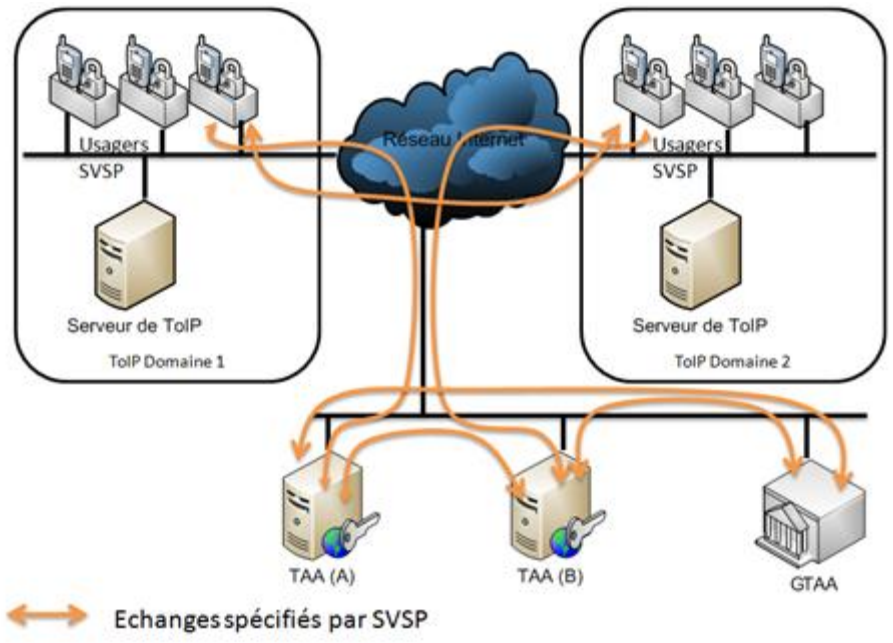


Figure 63. Architecture matérielle de SVSP

La sécurisation des messages est assurée par des certificats pour les échanges au niveau des TAA et des GTAA, et par un secret pré-partagé entre les TAA et les usagers. L'authentification mutuelle entre les entités est la brique de sécurité élémentaire de cette architecture. Cette disposition est largement justifiée par les travaux présentés dans ce manuscrit. Le GTAA est l'entité de confiance racine qui gère un ensemble de TAA. Il fournit les certificats, gère la base de révocation et assure les relations avec les autres GTAA. Les TAA délivre un identifiant unique et universel associé à un secret pour ses abonnés. Au cours d'un appel, il participe à l'élaboration d'une clé de session et au rapport de fin d'appel.

Les propriétés de sécurité offertes sont :

- pour la signalisation entre l'usager et le TAA :
    - l'authentification mutuelle ;
    - le non-rejeu ;
    - l'intégrité ;

- pour les échanges entre usagers :
    - l'authentification mutuelle des usagers ;
    - la confidentialité de la conversation et d'une partie de la signalisation ;
    - l'intégrité ;
    - le non-rejeu ;
    - la non répudiation de l'appel fournie sous la forme d'un rapport émis et signée par la TAA de l'usager.

Comme pour FNBDT, l'établissement de l'appel sécurisé se fait au travers d'échange de messages (cf. figure 64). Le déroulement du protocole SVSP débute une phase d'initialisation par l'envoi des messages en clair ou en chiffré comme : U_RUCA.req, U_RUCA.rep, etc. Ils permettent l'authentification des entités et l'échange des capacités cryptographiques. Pendant l'établissement de l'appel sécurisé, la clé de session est établie à partir du secret de l'usager qui initie l'appel et d'un nombre aléatoire généré par son TAA. Les TAA permettent l'authentification mutuelle des usagers. A l'issue, ces derniers vérifient certains paramètres et réalisent des acquittements permettant le passage en mode chiffré. La conversation est alors chiffrée à partir d'une clé de session, ainsi qu'une partie de la signalisation. Pour terminer une session, les usagers génèrent les messages dits « EndSecureMediaSession » (ESMS). A partir de ces derniers, les TAA génèrent les rapports de non-répudiation. La méthode de génération de la clé de session n'est pas imposée. Par ailleurs tous les messages font l'objet d'un contrôle d'intégrité par une fonction de hachage. Ils possèdent également tous un numéro de séquence et un horodatage. La chronologie d'un appel SVSP avec deux TAA est illustrée par la figure 64.

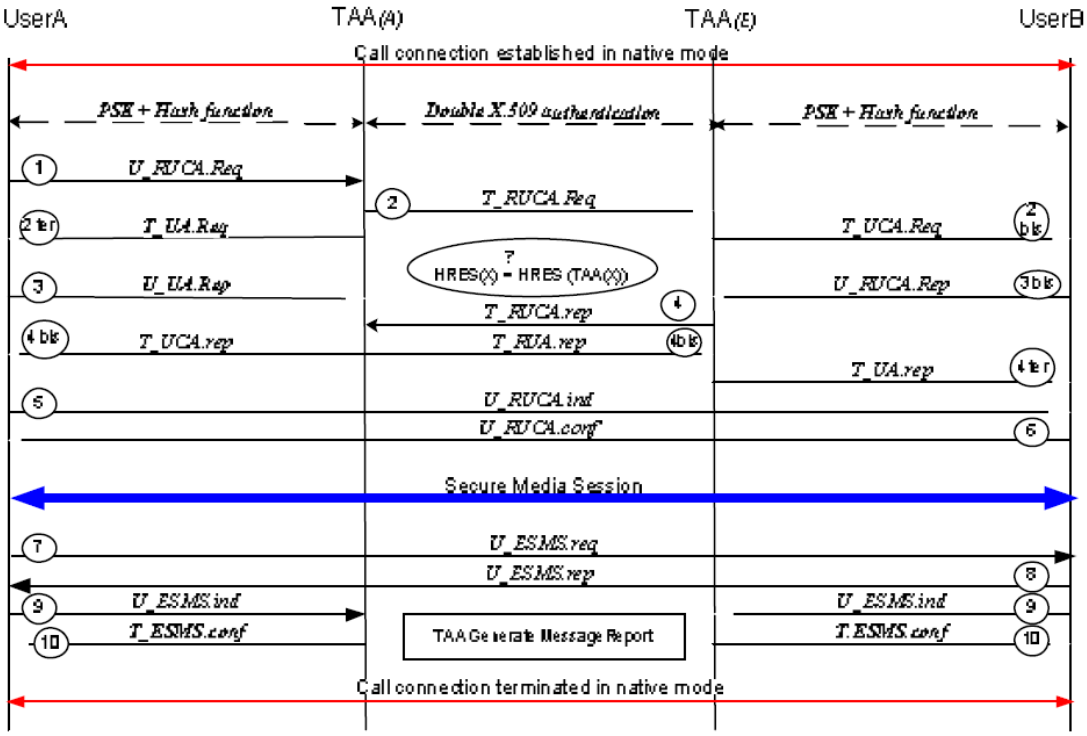


Figure 64. Scenario d'appel SVSP [BAS05]

Notre analyse de SVSP nous amène à mettre en avant les éléments suivants :

- il prévoit nativement une authentification mutuelle, ce qui limite les attaques de type « l'homme au milieu » ;
- il prévoit le chiffrement d'une partie de la signalisation ;
- il spécifie une architecture support pour la sécurité. Les entités appelées « Trusted Authentication Autority » et GTAA « Global Trusted Authentication Autority » permettent de garantir l'interopérabilité des authentifications ;
- il ne prévoit cependant pas de fiabilisation de la transmission, ce qui peut poser des problèmes avec une couche transport implémentant UDP.

SVSP a été validé dans certaines configurations mais n'a pas été déployé à grande échelle. Ce travail reste une des rares contributions à la sécurité de bout-en-bout de la téléphonie indépendante de la signalisation. La fiabilisation reste l'axe principalement d'amélioration de ce protocole.

### 6.2.3. *Comparaison entre les solutions de sécurité de bout-en-bout*

Dans ce manuscrit, nous avons analysé plusieurs mécanismes de sécurité. Pour bien percevoir l'intérêt des solutions de sécurité basée sur le canal média, une comparaison de plusieurs approches a été réalisée au travers du tableau 16. L'analyse confirme l'état des lieux présentée dans [§6.1.]. Seules les solutions type FNBDT ou SVSP garantissent une sécurité de bout-en-bout totalement interopérable. Certes ces protocoles ne spécifient pas la signalisation d'appel, mais ils interviennent en support pour la protection des appels. Il reste que les spécifications de la solution opérationnelle FNBDT ne sont pas publiques, ni destinées à usage civil, d'où l'intérêt de définir une solution ouverte pour les particuliers.

Tableau 16. Comparaison des solutions de sécurité bout-en-bout pour la ToIP

| Protocoles | SCIP FNBDT | SIP + S/MIME | SIP + SAML | SVSP | SRTP | Skype |
|---|---|---|---|---|---|---|
| Concerne : | | | | | | |
| Signalisation d'appel | Non | Oui | Oui | Non | Non | Oui |
| Voix | Oui | Non | Non | Oui | Oui | Oui |
| Propriété de sécurité | | | | | | |
| Confidentialité | Oui | Oui | Non | Oui | Oui | Oui |
| Intégrité | Non | Oui | Non | Oui | Oui | - |
| Authentification | Oui | Oui | Oui | Oui | Oui | Oui |
| Non rejeu | Oui | Non | Oui | Oui | Oui | - |
| Non répudiation | Non | Oui | Non | Oui | Non | - |
| Infrastructure de sécurité | PKI | PKI | PKI | PKI & PSK | PKI ou PSK | PKI |
| Interopérabilité | Totale (par conception) | Limitée aux usagers SIP | Limitée aux usagers SIP | Totale (par conception) | Flux RTP de bout-en-bout Nécessite une mécanisme de négociation de clé compatible avec la signalisation | Limitée aux usagers Skype |
| Standard | Oui | Oui | Non | Non | Oui | Non |
| Spécifications | Non publiques | Publiques | Publiques | Publiques | Publiques | Non publiques |

### 6.2.4. *Ce qu'il faut maintenir ou corriger pour définir une nouvelle architecture*

De l'analyse des solutions FNBDT et SVSP, nous retenons les éléments suivants pour la spécification d'une solution concurrente :

- spécifier une architecture support dédiée à la sécurité ;
- établir une signalisation de sécurité entre usagers dans le canal média ;
- chiffrer la signalisation dès qu'une clé de session est établie ;
- dans le cadre de la ToIP prendre en compte les spécificités des réseaux IP : latence, gigue, problème de fragmentation ;
- prévoir un mécanisme de fiabilisation pour le transport. La voix sur IP utilise généralement le protocole UDP ;
- retenir la chronologie d'un appel sécurisé spécifié par SVSP ;
- prendre en compte la notion d'interface avec l'existant : réseau IP, téléphone IP ;
- définir une application sous forme de modules ;
- prévoir un mécanisme d'intégrité ;
- définir les services de sécurité propres à chaque appel ;
- prévoir une authentification mutuelle des différentes entités avant l'établissement d'une connexion, surtout si une partie de la signalisation de sécurité est en clair.

## 6.3. Spécifications d'une architecture de téléphonie sur IP sécurisée

### 6.3.1. *Une architecture support dédiée à la sécurisation*

La définition d'une architecture de téléphonie sur IP sécurisée proposée est destinée à protéger les appels. La sécurité de bout-en-bout telle qu'elle est souhaitée peut s'envisager de deux manières soit dans la signalisation d'appel, soit dans le canal média. Le besoin d'interopérabilité sous-jacent ne permet pas à l'heure actuelle de s'appuyer sur la signalisation compte tenu de l'hétérogénéité des solutions techniques [BAS06]. Le choix du canal média est donc celui que nous avons retenu. Cette option sous-tend une architecture dédiée à la sécurité. Pour cela, l'analyse des solutions comme FNBDT, SCIP ou SVSP nous permet de définir trois entités distinctes :

- l'application de sécurité (AS) : elle s'interface avec le téléphone sur IP et permet la protection des appels et les échanges avec le tiers de confiance ;
- le tiers de confiance (TC) : il permet aux usagers au travers de l'application de sécurité de sécuriser les appels ;
- l'autorité de coordination (AC) : elle garantit l'interopérabilité entre les tiers de confiance.

Le tiers de confiance peut être considéré comme un fournisseur de service. Il fournit à l'usager les éléments secrets. Lorsqu'un client souhaite établir un appel sécurisé, il recherche le tiers de confiance de l'appelé pour créer une relation permettant la création d'une clé de session. Cela nécessite des identifiants standardisés : cette problématique n'est pas traitée dans ce manuscrit.

L'usager quant à lui doit posséder une téléphonie IP et l'application de sécurité pour permettre le déploiement de la solution de sécurité. L'application de ToIP permet l'établissement de l'appel et donc la mise en place du canal média. L'application de sécurité établit tout d'abord une connexion avec le tiers de confiance pour générer les secrets nécessaires à la protection de l'appel, puis génère une signalisation de sécurité entre usagers au travers du canal média.

L'autorité de coordination gère un groupe de tiers de confiance et les relations avec les autres autorités. Dans le cas d'emploi de certificats, elle est responsable du stockage, de la mise à jour de la liste des certificats périmés. Elle peut fournir à une autre AC le certificat d'un TC de sa responsabilité. Cette autorité a un rôle d'arbitrage et de contrôle de l'application de la politique de sécurité par les tiers de confiance. Une AC pourrait tout être un service étatique (ex. un régulateur).

La figure 65 présent cette architecture au niveau applicatif. Trois types d'échanges sont présents :

- la signalisation d'établissement d'appel pour la mise relation des usagers (cf. le fonctionnement de SIP ou H323). Elle se situe entre les différentes entités propres à la ToIP ;
- le canal média entre les usagers ;

- la signalisation de sécurité transportée directement par le réseau ou encapsulée dans le canal média.

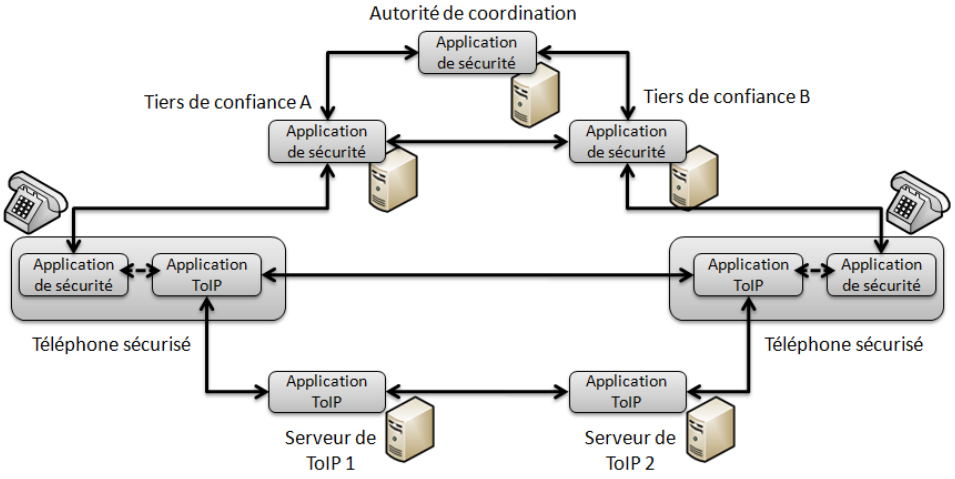


Figure 65. Echanges au niveau applicatif

Le tiers de confiance n'est pas forcément lié au fournisseur de téléphonie sur IP. Ce dernier doit être vu comme un fournisseur de services. De même le choix de l'application de ToIP est libre, la seule obligation est de pouvoir s'interfacer logiquement et/ou physiquement pour permettre les échanges nécessaires avec l'application de sécurité. Cette architecture est le socle physique et organisationnel indispensable pour faire émerger une solution de sécurité universelle pour la téléphonie sur IP. D'ailleurs deux usagers peuvent directement établir un appel sécurisé s'ils partagent déjà un secret.

### 6.3.2. *Les propriétés de sécurité d'un appel téléphonique*

Les propriétés de sécurité d'un appel téléphonique n'ont pas été définies. L'usager doit pouvoir spécifier ses besoins de sécurité. Comme cela a déjà été mentionné, la sécurité rajoute du temps de calcul cryptographique, une augmentation de l'occupation de la bande passante, du délai dans la transmission des paquets voix. Le mécanisme de protection doit donc être modulable pour ne pas rajouter des coûts dont l'utilité n'est pas avérée. Néanmoins deux propriétés nous paraissent indispensables quelques soient le contexte, l'authentification mutuelle des entités dans l'architecture sécurisée et le non rejeu. L'analyse de ce travail démontre sans ambigüité l'intérêt d'avoir la garanti de dialoguer avec la bonne entité. Pour le non rejeu, la garantie que les échanges ne puissent pas être réutilisés est également primordiale dans les réseaux ouverts comme Internet où les trafics peuvent être interceptés aisément.

Quant aux propriétés de sécurité comme la confidentialité, l'intégrité ou la non répudiation, elles ne nous semblent pas être nécessaires pour tous les appels téléphoniques. La confidentialité n'est pas nécessaire dans tous les cas comme pour une simple demande d'informations concernant une heure d'ouverture d'une administration. De même la non répudiation et l'intégrité ne sont pas forcément indispensable pour réserver une table au restaurant. Le niveau de sécurité doit être adapté chaque appel, limitant ainsi l'impact de la sécurité sur la QoS et l'occupation du réseau.

Cette architecture ouvre également de nouvelles perspectives dans le domaine de l'anonymat. La session voix pourrait être établie entre l'usager et le tiers de confiance. Au travers de la signalisation de sécurité le numéro de l'appelé peut être protégé en confidentialité. L'appel vers le destinataire final serait alors masqué par l'ensemble des connexions établies à partir du tiers de confiance. L'infrastructure suggérée permet une anonymisation des associations appelant/appelé.

### 6.3.3. *Le déroulement d'un appel téléphonique sécurisé de bout-en-bout*

La mise en relation des entités définies précédemment nécessite un séquencement dans les différentes connexions. Après l'établissement de l'appel dont le principe a déjà été établi dans le début du manuscrit, les usagers initie l'appel sécurisé en sollicitant leur tiers de confiance pour obtenir la clé de session. Chaque usager fournit son identifiant, celui du correspondant, les capacités cryptographiques et les propriétés de sécurité souhaitées. Ce principe est établi dans de nombreux protocoles comme SIP [RFC3261] qui fournit dans ses messages le « From », le « To » et ses capacités d'échange au travers du protocole SDP [RFC4568].

Les tiers de confiance se mettent en relation selon un modèle qui peut s'apparenter à celui de la téléphonie. Ils négocient la clé de session et la compatibilité des besoins de sécurité. Dès lors que les applications de sécurité possèdent la clé de session, ils peuvent échanger directement entre eux au travers du canal média. La figure 66 décrit de manière les échanges.

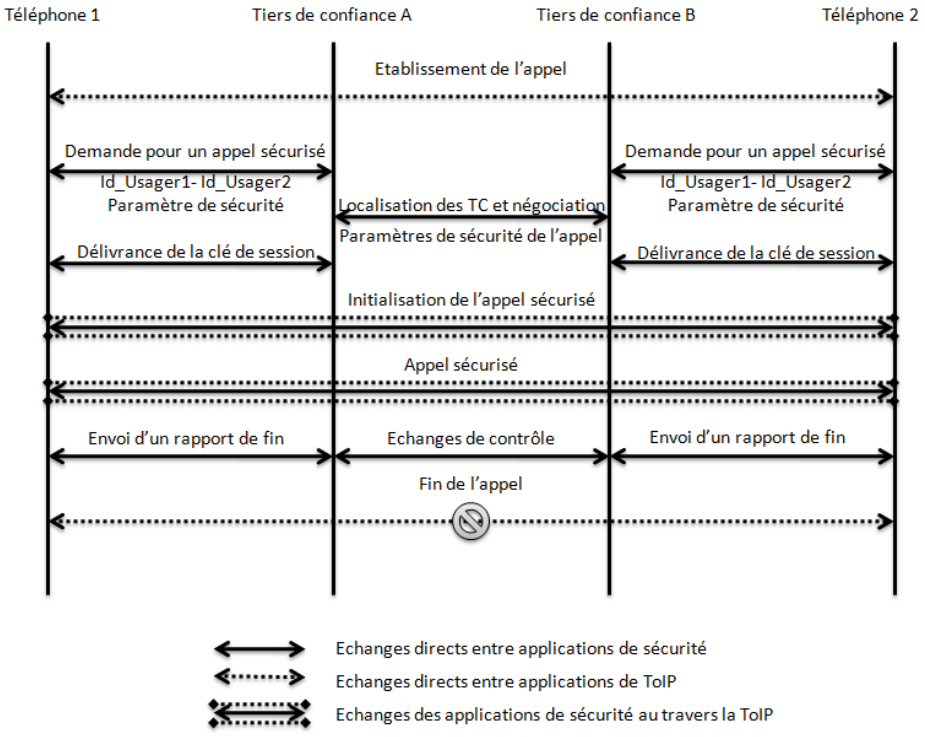


Figure 66. Etablissement d'un appel sécurisé

Les relations de confiance qui existent entre les différentes entités doivent permettre de générer une clé de session et de la diffuser de manière sécurisée. Un attaquant qui écoute

le réseau ne doit pas pouvoir trouver le secret qui sécurise l'appel. Dans la mesure où les usagers possèdent un secret pré-partagé, la sollicitation des tiers de confiance n'est pas forcément nécessaire. Les usagers peuvent passer directement de l'établissement d'appel à l'initialisation de l'appel sécurisée mais toutes les propriétés de sécurité ne pourront pas être garanties.

### 6.3.4. *Une architecture protocolaire*

Pour mettre en œuvre cette architecture, nous définissons une pile protocolaire cohérente avec les architectures de téléphonie sur IP. Le niveau de spécification est celui d'une analyse fonctionnelle. La pile protocolaire présentée identifie les composants logiques et les contraintes. Chaque composant est recensé, caractérisé, ordonné, hiérarchisé et valorisé. Le recensement des contraintes permet par ailleurs un dimensionnement adéquat. L'objectif est de fournir les éléments nécessaires à la réalisation de cette solution.

L'architecture type d'une solution de ToIP est illustrée par la figure 67. La sécurité applicative proposée devra s'interfacer au niveau du protocole de diffusion de la voix. Ce dernier est généralement associé à UDP [RFC768] qui est un protocole de transport fonctionnant en mode non-connecté : il n'y a pas de moyen de vérifier si tous les datagrammes envoyés sont bien arrivés à destination et ni dans quel ordre. Il n'est prévu aucun contrôle de flux ni contrôle de congestion. C'est pour cela qu'il est souvent décrit comme étant un protocole non-fiable. Cette caractéristique devra être prise en compte dans notre architecture au travers d'un mécanisme de fiabilisation.

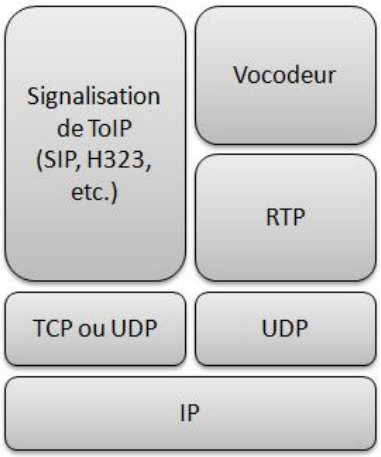


Figure 67. Architecture protocolaire générique d'une solution de ToIP

L'appel sécurisé prévoit une signalisation de sécurité et une protection du canal média. La pile protocolaire doit donc intégrer un vocodeur, un module de gestion de la signalisation, un module cryptographique. Par ailleurs comme nous l'avons précisé précédemment, le besoin de sécurité doit être adapté à chaque appel. Il faut donc également un module pour gérer les propriétés de sécurité demandées. La pile protocolaire (cf. figure 68) s'appuie sur deux types de protocoles sous-jacents :

- le protocole RTP pour la diffusion de la voix, lui-même s'appuyant sur UDP. Le canal média doit donc être considéré comme non fiable pour le transport de la signalisation ou la voix générées par l'application de sécurité entre les usagers ;
- le protocole de transport du réseau IP est soit TCP ou UDP. Dans la mesure où le canal média est considéré non fiable, nous considérons UDP pour le transport de la signalisation entre les usagers et les tiers de confiance. Cette considération sous-entend qu'un mécanisme de fiabilisation est systématiquement assuré par l'application de sécurité.

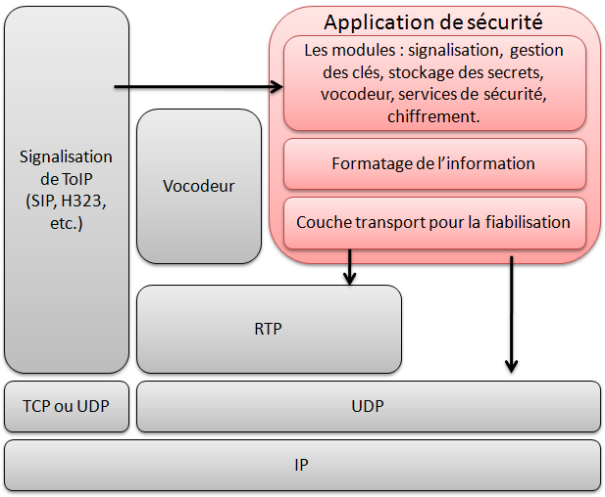


Figure 68. Pile protocolaire de la signalisation de sécurité

La pile protocolaire (cf. figure 68) se décompose en trois couches :

- la couche « Modules » :
  - le module signalisation : il permet les connexions avec le tiers de confiance et l'établissement de l'appel sécurisé avec un autre usager. IL doit accéder à l'identifiant de l'appelant et de l'appelé pour les fournir au tiers de confiance ; Ces informations sont données par le protocole de signalisation de ToIP, soit par le module « service de sécurité » ;
  - le module de chiffrement : il effectue les opérations de chiffrement et de déchiffrement en utilisant les éléments secrets du module « gestion des clés » ;
  - le module de gestion des clés : il stocke le secret fourni par le tiers de confiance, la clé de session, et éventuellement une clé pré-partagé entre usagers ;
  - le module services de sécurité : il fournit à l'établissement de l'appel sécurisé les propriétés de sécurité souhaitées par l'usager. Si une interface n'est pas possible entre l'application de sécurité et celle de ToIP, ce module reçoit les identifiants de l'appel ;
  - le vocodeur : il fournit un vocodeur à l'application de sécurité, ce qui limite l'interface avec le téléphone IP ;
- la couche « Formatage » : elle permet la mise en forme des données selon les spécifications de la signalisation ;

- la couche transport : elle fiabilise le transport. Le média est généralement transporté par UDP qui ne garantit pas la réception des paquets.

Cette pile prévoit des échanges avec d'autres éléments. Trois interfaces ont été identifiées :

- avec la couche transport UDP ;
- avec le protocole de diffusion de la voix (principalement RTP) ;
- avec la signalisation de ToIP pour obtenir les identifiants de l'appelant et de l'appelé.

Tableau 17. Qualité d'écoute en fonction du délai de transmission [DEO07]

| Délai de transmission de la voix | Qualité d'écoute |
|---|---|
| < à 300 ms | Excellente |
| Entre 300 et 500 ms | Moyenne |
| Entre 500 ms et 1 s | Faible |
| > à 1 s | Impossible |

Enfin les délais de transmission doivent être compatibles du besoin d'une application synchrone avec des contraintes temporelles comme le téléphone. Le tableau 17 donne la qualité d'écoute en fonction des temps d'acheminement de la voix. Les temps de calcul cryptographique et le volume d'informations à traiter pour sécuriser l'appel devront être compatibles avec ces délais de transmission. Cette considération devra être prise en compte dans la conception de la signalisation mettant en œuvre cette architecture.

## 6.4. Conclusion

L'architecture définie dans ce chapitre est dédiée à la sécurité des appels. Elle garantit une protection de bout-en-bout en utilisant le canal média pour mettre en œuvre une signalisation de sécurité. Notre approche ne nécessite pas de modifications des infrastructures déjà déployées. Compte tenu de l'hétérogénéité des solutions de ToIP, cette totale interopérabilité avec l'existant est l'élément décisif pour son adoption à grande échelle.

La faisabilité de cette approche a été démontrée par FNBDT et SVSP. Notre analyse de ces solutions nous a permis de définir une nouvelle architecture entérinant certains choix, et en corrigeant d'autres. Nous avons confirmé la nécessité d'avoir une authentification mutuelle entre chaque entité dans le contexte de la ToIP. La fiabilisation du transport a également été mis en avant dans notre conception en identifiant dans la structure protocolaire une couche dédiée à cet objectif. Nous avons enfin établi les différents flux d'informations, confirmant le besoin d'une architecture support dédiée à la sécurité.

Il reste à décliner cette architecture au niveau des échanges protocolaires.