Etat de l'art de la sécurité sur ATM [1]

Maryline LAURENT[2], Pierre ROLIN
Télécom Bretagne
rue de la châtaigneraie - BP 78
35512 CESSON Cedex - France
E-mail : {mlaurent,rolin}@rennes.enst-bretagne.fr

Résumé. Cet article présente un état de l'art des solutions visant à assurer la sécurité des communications sur les réseaux ATM. Il analyse les différentes solutions, les compare et précise, pour chacune d'entre elles, les services de sécurité offerts, leur placement au sein du modèle de référence du protocole ATM, les mécanismes utilisés pour négocier ces services de sécurité et les techniques pour résoudre les problèmes de synchronisation et de changement de clés dynamique qui se posent lors de l'échange de données utilisateur.

Mots-clés : RNIS-LB, ATM, sécurité des réseaux, services de sécurité.

Abstract. *This paper presents a survey of existing solutions aiming to secure communications over ATM networks. Different solutions are analyzed and compared. Details are given about the security services offered, their placement within the ATM Protocol Reference Model, the mechanisms to negotiate security services and the techniques to provide synchronization and dynamic key change during user data exchange.*

Keywords : B-ISDN, ATM, network security, security services.

1. Introduction

Du fait de l'importance des débits offerts et de leur capacité à transporter des données de tout type (voix, données, images, vidéo), les réseaux ATM (*Asynchronous Transfer Mode* en anglais) sont considérés comme les réseaux qui, demain, assureront le transport de données de bout en bout et permettront aux utilisateurs d'accéder, au travers d'un unique interface réseau, à des applications de communication diverses telles que l'imagerie, la vidéoconférence, la télécopie, etc. Cependant, malgré tous les avantages offerts par cette technologie, l'introduction de l'ATM risque d'être gênée dans les secteurs qui nécessitent l'échange d'informations sensibles telles que les transactions bancaires, les dossiers médicaux. En effet, du fait qu'aucun service de sécurité n'est actuellement disponible sur les réseaux ATM, les échanges de données ne sont pas protégés sur ces réseaux et peuvent être la cible d'attaques malintentionnées variées ([Lau95],[Lau96]). Pour les échanges d'informations sensibles, cela peut avoir de graves conséquences puisqu'un individu malveillant posté en un point du réseau ATM et muni d'un analyseur de trafic peut réussir à prendre connaissance du montant d'une transaction effectuée par un tel ou pire encore, il peut modifier la valeur du montant de cette transaction.

Actuellement, plusieurs travaux ([Ste95],[Den95],[Chu96],[AFSEC],[Pau96]) portent sur l'inté-

---

1. Dans les actes de 1996 du onzième Congrès «De Nouvelles Architectures pour les Communications» (DNAC'96); Versailles.
2. Ce travail est financé par la DRET.

gration de services de sécurité (au sens [X800], cf. annexe 2) dans le modèle de référence ATM-présenté section 2. Cet article vise à décrire et comparer les différentes approches considérées. Pour cela, chaque approche est étudiée sous les deux aspects correspondant aux deux étapes nécessaires pour assurer la sécurité d'une communication, c.à.d : **(1)** la négociation préliminaire d'un **contexte de sécurité** (services de sécurité, algorithmes et clés de chiffrement) et **(2)** l'application des services de sécurité négociés aux échanges de données et éventuellement de messages de signalisation. Ces deux aspects font l'objet des sections 3 et 4.

Toutes ces approches sont résumées à la fin de l'article tableaux 2 et 3. Quelques conclusions sont présentées section 5.

2. Le modèle de référence ATM

Comme le montre la figure 1, le modèle de référence ATM ([Pry91],[I321]) comprend trois plans :

- le plan utilisateur qui permet l'échange de données utilisateur,
- le plan de contrôle qui gère les informations de signalisation (ouvertures/fermetures de connexions),
- le plan de gestion chargé de maintenir le réseau opérationel.

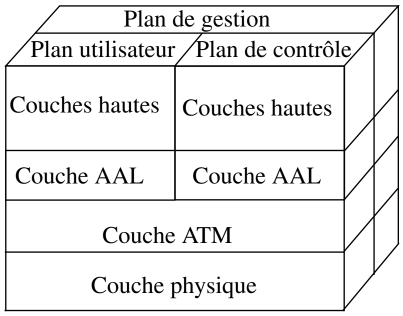

Figure 1 : Modèle de référence du protocole ATM

Le plan de contrôle communique au travers du réseau ATM par le biais de canaux virtuels réservés. Le plan de gestion peut utiliser le même canal que le plan utilisateur pour échanger des cellules de gestion OAM (*Operation And Maintenance*) permettant de mesurer diverses caractéristiques de service. Toutes les informations sont échangées sur le réseau sous forme de cellules ATM de 53 octets.

Le modèle ATM comprend trois couches basses : une couche physique principalement responsable de la transmission sur le réseau, une couche ATM essentiellement chargée des fonctions de multiplexage et de commutation et une couche AAL (*ATM Adaptation Layer*) qui permet entre autre d'adapter les besoins des applications aux flux ATM en effectuant par exemple des segmentations/réassemblages de cellules ATM.

3. La négociation des services de sécurité

Trois approches sont considérées jusqu'à présent. Elles se différencient suivant que la négociation du contexte de sécurité[1] :

- fait partie intégrante de l'ouverture de connexion ([AFSEC],[Den95],[Chu96],[Pau96])
- s'effectue en continu en tant qu'informations de gestion ([AFSEC])
- fait l'objet d'une connexion spécifique ([Ste95],[AFSEC])

La solution choisie par l'ATM Forum [AFSEC] se sert de chacune de ces approches pour échanger des informations de sécurité.

Les notations utilisées pour décrire les approches sont indiquées tableau 1.

1. Voir la définition des services de sécurité annexe 2.

A	entité appelante
B	entité appelée
KAB	clé de session à utiliser pour chiffrer les données de A vers B
KsA {M}	message M chiffré avec la clé privée de A
KpA{M}	message M chiffré avec la clé publique de A
T_A	horodateur généré par A
N_A	nonce (i.e. nombre aléatoire) émis par A
CA	entité de certification
Cert_A	certificat de la clé publique de A certifié par CA

Tableau 1 : Notations

3.1. Négociation par le biais d'informations de signalisation

Cette approche consiste à placer dans les messages de signalisation d'ouverture de connexion SET UP[1] et CONNECT [2] des informations de sécurité (clés de chiffrement, mécanismes de sécurité, authentificateur). En général, des Eléments d'Information[3] (IE en anglais pour *Information Element*) de sécurité sont ajoutés à ces messages.

3.1.1. La solution ATM Forum [AFSEC]

L'ATM Forum définit sept nouveaux IEs pour réaliser de l'authentification (1 IE), du contrôle d'accès (1 IE), l'échange de clés de session unidirectionnelles (1 IE) et la négociation d'un contexte de sécurité (4 IEs). Ces différents IEs de sécurité sont décrits ci-dessous.

3.1.1.1. Le service d'authentification

Le format de l'IE d'authentification est donné figure 2. Il permet d'authentifier l'émetteur du message de signalisation par la validation de la signature digitale placée dans l'IE. L'ATM Forum distingue trois types d'authentification suivant que l'authentification est effectuée de bout en bout (entre terminaux), entre commutateurs ou entre terminaux et commutateurs. L'ATM Forum encourage l'utilisation de cet IE non seulement dans les messages d'ouverture de connexion (SET UP et CONNECT) mais également dans d'autres messages tels que ceux de libération de connexion.

En plus du service d'authentification, l'IE permet d'assurer l'intégrité d'une portion ou de tout le message de signalisation afin de déceler les éventuelles modifications survenues au cours de son transfert. Il permet également de détecter, grâce aux champs *Sequence number* et *Timestamp*, les rejeux de messages (précédemment authentifiés) qu'une personne pourrait réaliser dans le but d'usurper l'identité d'une autre personne auprès d'un tiers.

Tel qu'il est défini figure 2, l'IE d'authentification apparaît imprécis et imparfait.

(1) Il n'est pas optimisé en ce sens qu'un commutateur doit systématiquement pour chaque message de signalisation reçu analyser les champs de l'IE d'authentification jusqu'au bit *E/E* pour sa-

1. SET UP est envoyé par A pour demander une ouverture de connexion avec B.
2. CONNECT est envoyé par B en réponse à un SET UP pour indiquer à A que la connexion est acceptée.
3. Les messages de signalisation sont structurés en éléments d'information qui contiennent chacun un type d'information utile aux opérations de contrôle. Par exemple, dans les messages SET UP, il existe des IEs contenant les adresses ATM de A et B qui sont appelés *calling and called entity number IEs*.

Authentication IE Identifier	
	IE instr. field
Length	
Version	
E/E		Signature algorithm
Sequence number	
Timestamp (4 bytes)	
IE list lenth	
IE list	
Reserved	
Algorithm-specific information	
Signature	

L'IE d'authentification comprend (cf. [AFSEC] pour les détails):
- *Authentication IE Identifier* identifie l'IE d'authentification dans le message de signalisation
- *Length* la longueur de l'IE d'authentification
- *Version* définit le numéro de version des spécifications auxquelles se conforme l'IE
- le bit *E/E* (ou *End-to-End*) distingue les IEs d'authentification de bout en bout (*E/E*=1) des IEs d'authentification entre terminaux et commutateurs ou entre commutateurs (*E/E*=0)
- *Signature algorithm* contient la référence de l'algorithme utilisé pour signer
- *Sequence number/timestamp* permettent de rendre unique chaque IE d'authentification
- *IE list length* et *IE list* précisent respectivement le nombre d'IEs constituant la liste d'IEs et la liste ordonnée des identificateurs d'IEs (ordre dans lequel les IEs doivent être chiffrés) sur lesquels la signature digitale doit porter.
- *Algorithm-specific information* permet d'inclure ici des informations propres à la validation de la signature
- *Signature* contient la signature digitale calculée sur les IEs listés dans l'ordre dans *IE list* et sur le contenu de l'IE d'authentification

Figure 2 : L'IE d'authentification pour la solution ATM Forum

voir s'il doit réaliser une authentification (*E/E*=0) ou non (*E/E*=1). Il serait beaucoup plus performant de distinguer les IEs d'authentification de bout en bout des autres IEs en leur attribuant des identificateurs d'IE différents. Ainsi les commutateurs limiteraient leur analyse aux seuls IEs d'authentification dont ils doivent vérifier la signature.

(2) D'autre part, avec cet IE, seule une authentification portant sur les terminaux émetteur et récepteur (leurs adresses) est possible du fait qu'aucun champ n'est prévu pour identifier plus précisément l'émetteur/récepteur du message.

(3) De plus cette authentification n'est pas fiable en ce sens qu'il existe un scénario qui permet d'émettre des données d'un terminal espion en faisant croire qu'elles proviennent d'un terminal intègre. En effet supposons que le terminal A s'authentifie auprès du terminal B avec un IE d'authentification dont la signature ne porte pas sur les IEs d'adresses ATM de A et B. Un intrus (un individu placé en écoute sur le réseau ou même sur le terminal B) peut récupérer l'IE d'authentification de A et le rejouer auprès d'un terminal C pour faire croire à ce dernier qu'il travaille sur A. Comme l'IE d'authentification n'inclut aucune information sur l'adresse du destinataire B, cette attaque est possible, mais elle suppose bien entendu que le champ *Sequence number* ait une valeur appropriée et que l'intrus rejoue suffisamment rapidement l'IE pour que le champ *Timestamp* reste valide.

Le champ *version* permet que de nouveaux IEs d'authentification puissent être développés et même simultanément exploités sur le même réseau.

3.1.1.2. Les services de négociation de services de sécurité et d'échange de clés

L'ATM Forum définit cinq types d'IEs de sécurité (cf. figure 3) dont l'échange permet de mettre en place les services de confidentialité et d'intégrité (qui serviront à protéger l'échange ultérieur de données), le service d'authentification et les services d'échange et de renouvellement des clés. Ces services de sécurité peuvent être mis en place de bout en bout (entre terminaux) ou entre commutateurs, ce qui permet de protéger les connexions ATM de bout en bout ou sur des segments du réseau.

- IE#1 contient les options de sécurité que l'émetteur du message souhaiterait appliquer, à savoir les services de sécurité à négocier avec, pour chacun d'eux, l'algorithme préférentiel choisi, le protocole de négociation de services de sécurité (à deux ou trois échanges), les algorithmes d'échange de clés et de renouvellement de clés.

- IE#2 contient un second choix possible d'options de sécurité pour réaliser les services de sécurité. Elles pourront être choisies par B si les options précisées dans l'IE #1 ne lui conviennent pas.

- IE#3 permet d'authentifier l'émetteur du message de signalisation, avec un format d'IE assez proche de celui de l'IE d'authentification décrit section 3.1.1.1.

- IE#4 est utile au fonctionnement du protocole de négociation à trois échanges du fait qu'il permet à B de signaler à A qu'il attend un troisième message de signalisation (CONNECTION AVAILABLE) de sa part.

- IE#5 permet de communiquer trois clés : les deux clés de session à utiliser pour rendre les services de confidentialité et d'intégrité des données et une clé maître $K_{m,AB}$ qui permettra de renouveler au cours de la connexion le jeu de clés de session en assurant leur chiffrement. Cet IE est bien entendu protégé en confidentialité par l'algorithme spécifié dans l'IE#1.

Figure 3 : Les IEs de sécurité pour la solution ATM Forum

Ces IEs de sécurité sont échangés dans la signalisation suivant des protocoles de sécurité basés sur des algorithmes à clés symétriques ou asymétriques nécessitant deux voire trois échanges. En fait, les spécifications [AFSIG] relatives à la signalisation ATM définies par l'ATM Forum limitent actuellement les ouvertures de connexion à deux messages de signalisation (SET UP, CONNECT), alors que le groupe sécurité de l'ATM Forum propose d'introduire un message de signalisation supplémentaire CONNECTION AVAILABLE en se basant sur les travaux réalisés par l'ITU-T [Q2963]. Avec ce troisième message de signalisation, il est alors possible d'implémenter des protocoles de sécurité à trois échanges (en général plus fiables que les protocoles à deux échanges) pour mettre en place les services de sécurité et échanger des clés de façon sécurisée.

Compte tenu de l'état d'ébauche des spécifications ATM Forum [AFSEC], la définition des cinq IEs de sécurité comporte certaines imprécisions à savoir : l'IE#3 qui réalise de l'authentification fait double emploi avec l'IE d'authentification de la section 3.1.1.1 ; contrairement à l'IE d'authentification de la section 3.1.1.1, les IEs définis figure 3 ne contiennent aucune indication du type *E/E* dans [AFSEC] si bien qu'il est impossible de savoir si ces IEs permettent de faire de la négociation de services de bout en bout uniquement ou s'ils permettent également de négocier des services de sécurité entre deux commutateurs ATM.

3.1.1.3. Le service de contrôle d'accès

L'ATM Forum définit un IE spécifique au contrôle d'accès qui permet de spécifier dans le message d'ouverture de connexion, le niveau de sensibilité des données à échanger sur la connexion. Selon le niveau de sensibilité mentionné («public», «confidentiel», «limité à l'entreprise», etc.), l'ouverture de connexion sera satisfaite s'il existe un chemin pour lequel tous les segments de réseau présentent des niveaux de sensibilité suffisants.

3.1.2. La solution Robert H. Deng et al. [Den95]

Deng et al. définissent 12 nouveaux IEs - 6 pour chacun des messages SET UP et CONNECT - qui permettent l'authentification mutuelle, l'échange de deux clés de session unidirectionnelles (2 IEs) et la négociation d'un contexte de sécurité (4 IEs).

La négociation du contexte se limite aux deux services de confidentialité et d'intégrité à appliquer au flux de données. L'entité initiatrice de la connexion A propose dans les quatre premiers IEs du SET UP (IE#1 à #4 - cf. figure 4) un QoS de protection, une liste de paramètres à utiliser

Les IEs de sécurité que A doit inclure dans le SET UP :
IE#1: Identificateur de l'Association de Sécurité de A
IE#2: QoS de protection : type d'authentification, niveaux de confidentialité et d'intégrité
IE#3: Paramètres du service de confidentialité
IE#4: Paramètres du service d'intégrité
IE#9: Certificat de A Cert_A = KsCA{numéro de série, période de validité, A, KpA, CA}
IE#10: Jeton de A = KsA{TA, B, KpB{KAB}}

Les IEs de sécurité que B doit inclure dans le CONNECT :
IE#5: Identificateur de l'Association de Sécurité de B
IE#6: QoS de protection choisi : type d'authentification choisi, niveaux de confidentialité et d'intégrité choisis
IE#7: Paramètres du service de confidentialité choisis
IE#8: Paramètres du service d'intégrité choisis
IE#11: Certificat de B Cert_B = KsCB{numéro de série, période de validité, B, KpB, CA}
IE#12: Jeton de B = KsB{TA, A, KpA{KBA}}

Figure 4 : Les IEs de la solution de Deng

pour rendre les services de confidentialité et d'intégrité du flux de données. B retourne ensuite dans le CONNECT (IE#5 à #8) son QoS de protection et son choix de paramètres. Après réception du CONNECT, A accepte ou rejette la connexion suivant que le choix de B lui convient.

Le service d'authentification et l'échange de clé de session sont basés sur le protocole d'authentification X509 à deux échanges. Le premier message X509 placé dans le SET UP est constitué du certificat de la clé publique de l'entité émettrice (IE#9) qui permet à B de récupérer la clé publique de A et d'un jeton KsA{TA, B, KpB{KAB}}(IE#10) qui authentifie A et permet l'envoi à B d'une clé de session KAB de façon sécurisée. Le second message X509 placé dans le CONNECT (IEs #11 et #12) est identique.

Cette approche est rigide du fait que le protocole d'authentification est imposé. De plus l'idée d'attribuer un IE à chaque fonction de sécurité remplie rend la solution très structurée mais peu optimisée en termes de modifications à apporter aux spécifications [AFSIG].

3.1.3. La solution Shaw-Cheng Chuang [Chu96]

La solution proposée par Chuang s'inscrit dans l'architecture MSN-CMA (*Multi-Service Network Connection Management Architecture*) [Cros95] qui s'articule autour de serveurs chargés de toutes les opérations de contrôle (ouverture/libération de connexions) et de gestion (routage, réservations de ressources) effectuées sur le réseau ATM. C'est à dire, lorsque A veut ouvrir une connexion, il doit envoyer son message de signalisation au serveur adéquat par le biais de mécanismes RPC (*Remote Procedure Call*). Le serveur doit ensuite trouver le chemin approprié entre A et B, avertir B de la demande de connexion et positionner les tables de routage des commutateurs ATM correctement.

Pour cette solution, une ouverture de connexion nécessite l'échange de trois messages de signalisation au lieu des deux préconisés jusqu'ici par l'ATM Forum [AFSIG] et l'ITU-T. Cette particularité de l'établissement d'une connexion à trois passes sur MSNA apparaît très précieuse pour la négociation du contexte de sécurité du fait que de nombreux protocoles d'échanges de clés, en particulier ceux basés sur les nonces, s'effectuent en trois temps. Par le biais de ces messages d'ouverture de connexion, Chuang propose de négocier entre autres les services de confidentialité, d'intégrité et d'échange de clés qui permettront de protéger l'échange ultérieur de données.

Chuang propose également la possibilité de renégocier la politique de sécurité de la connexion via la signalisation par l'échange de trois messages supplémentaires.

3.1.4. La solution Télécom Bretagne [Pau96]

La solution Télécom Bretagne définit un nouvel IE de sécurité (cf. figure 5) proche de l'IE d'authentification de l'ATM Forum que nous avons décrit en section 3.1.1.1. Cet IE permet de négocier les services de sécurité - confidentialité, intégrité/authentification et bourrage - à appliquer ultérieurement aux échanges de données ainsi que le service de confidentialité à appliquer aux échanges de signalisation ultérieurs. Il permet d'authentifier l'émetteur du message de signalisation, de garantir l'intégrité et la confidentialité d'une partie du message et de détecter les rejeux de messages.

Ces services de sécurité peuvent être mis en place entre des terminaux ATM ou entre les commutateurs ATM de réseaux locaux distants qui désirent protéger leurs communications sur le réseau public. Cette solution est particulièrement bien adaptée lorsque les terminaux ou réseaux locaux - typiquement des entreprises et leurs filiales - sont amenés à fréquemment communiquer.

L'IE de sécurité est organisé en éléments de sécurité qui correspondent chacun à des services de sécurité rendus ou à négocier. Ces éléments de sécurité sont optionnels.

Les services de sécurité qui peuvent être rendus par cet IE sont détaillés ci-dessous :

- l'authentification et l'intégrité d'une partie du message
  Tout comme l'IE d'authentification de l'ATM Forum, l'IE de sécurité permet d'authentifier l'émetteur du message et de garantir l'intégrité de l'IE de sécurité et de la partie du message de signalisation spécifiée dans les champs *IEs list length* et *IEs list*. Le résultat de la signature est placé dans le champ *Digital Signature*.
  Contrairement à l'IE d'authentification, il est possible pour A et B de négocier l'algorithme de génération de la signature. Pour cela, A doit préciser dans le champ *List of algorithms to be used for signature* dans le SET UP, la liste des algorithmes disponibles dans l'ordre de préférence décroissant, le premier algorithme spécifié étant le code de l'algorithme utilisé pour générer la signature de l'IE de sécurité. Ainsi, si l'algorithme de génération de la signature ne convient pas à B, B peut choisir un autre algorithme de la liste et le communiquer à A par l'intermédiaire de 'IE de sécurité retourné dans le CONNECT. A devra alors utiliser cet algorithme pour s'authentifier dans les messages de signalisation suivants.

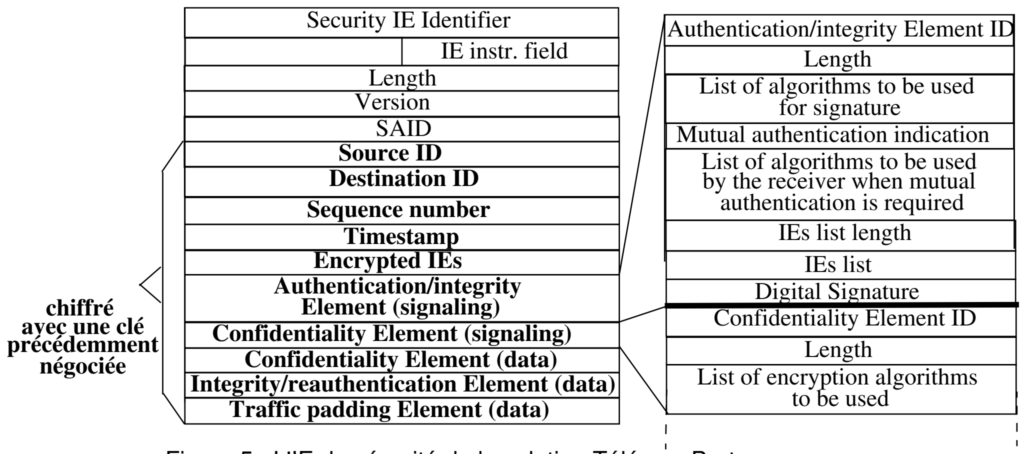

Figure 5 : L'IE de sécurité de la solution Télécom Bretagne

Avec cet IE de sécurité, A peut également exiger, par le biais du champ *Mutual authentication indication*, que B s'authentifie avec l'un des algorithmes spécifiés dans le champ *List of algorithms to be used by the receiver when mutual authentication is required*.
Contrairement à l'IE d'authentification de l'ATM Forum (cf. point (1) section 3.1.1.1), il est possible de réaliser une authentification sur les adresses des terminaux mais aussi sur l'identité des utilisateurs du fait que les champs *Station ID* et *Destination ID* peuvent servir à transporter les noms d'utilisateur ou des identificateurs de groupes (une autre possibilité d'utilisation de ces deux champs est décrite ci-dessous).

- la confidentialité d'une partie du message de signalisation
Ce service nécessite qu'un contexte de sécurité (i.e. clés et algorithmes de chiffrement) ait préalablement été négocié entre A et B (à l'aide des outils d'administration de la sécurité de réseau). Compte tenu du contexte considéré où A et B sont supposés communiquer fréquemment, il est tout à fait raisonnable de supposer que A et B aient déjà ouvert une connexion entièrement dédiée à la sécurité pour échanger de façon sécurisée un grand nombre de clés de session de telle sorte qu'à l'ouverture d'une connexion, aucun échange de clés n'est nécessaire. Ce contexte est identifié par un numéro ou SAID (pour *Secure Association Identifier*) qui permet aux entités communicantes, après réception d'un IE de sécurité, de facilement retrouver le contexte de sécurité adéquat et de déchiffrer l'IE avec la clé appropriée.
Cette approche permet de chiffrer une partie de la signalisation, i.e. la partie de l'IE de sécurité qui apparaît en caractères gras sur la figure 5 et certains IEs ordinaires qui, parce qu'ils ne sont pas analysés par le réseau public, peuvent être déplacés à l'intérieur de l'IE de sécurité dans le champ *Encrypted IEs* pour être protégés en confidentialité.
Cet IE de sécurité peut également servir à cacher des informations telles que les adresses ATM des terminaux. Cette solution s'avère particulièrement intéressante dans le cas d'entreprises désirant communiquer avec leurs filiales au travers du réseau public tout en maintenant secret le plan d'adressage de leur réseau interne. Pour cela, il suffit de définir une adresse globale pour l'ensemble des terminaux de l'entreprise. Cette adresse est la seule adresse à apparaître en clair dans les messages SET UP (dans le *called entity number IE*) lors de l'ouverture d'une connexion avec cette entreprise. Les véritables adresses des terminaux émetteur et récepteur sont chiffrées dans les champs *Source ID* et *Destination ID* de l'IE de sécurité, ce qui suppose bien entendu que le commutateur récepteur de l'entreprise serve de «passerelle» de sécurité ou firewall, en déchiffrant l'IE de sécurité avec le contexte de sécurité SAID adéquat avant de transmette le message déchiffré au bon terminal.

- la détection de tout rejeu de message de signalisation grâce aux champs *Sequence number* et *Timestamp*.

- la négociation des services de confidentialité (pour protéger les échanges de signalisation et de données), d'intégrité/réauthentification et de bourrage.
Quatre éléments de sécurité permettent à A et B de négocier les algorithmes, ainsi que les numéros de clés de session à utiliser pour mettre en place les services de sécurité correspondants. Pour cela, A doit spécifier, pour chaque service de sécurité négocié, une liste d'algorithmes possibles dans l'ordre de préférence décroissant. Après avoir sélectionné un algorithme dans cette liste, B doit communiquer à A son choix dans le message CONNECT. Il suffit alors, pour A et B, de mémoriser ce nouveau contexte de sécurité (identifié par SAID) en vue de l'appliquer aux échanges de signalisation ou de données utilisateur ultérieurs.

3.2. Négociation par le biais des informations de gestion

Cette approche consiste à introduire des informations de sécurité telles que la négociation de clés de session dans les flux de gestion OAM (cf. section 2). Elle a l'avantage d'assurer la synchronisation de ces informations de sécurité avec le flot de données utilisateur, ce qui permet par exemple de changer de clés de session en cours de chiffrement. Cependant elle est peu adaptée aux connexions de type CBR (*Constant Bit Rate*) car les informations de gestion introduites sont comptabilisées en tant que données utilisateur, et si elles sont échangées en quantités, elles peuvent affecter la qualité de service de la connexion. Pour pallier à ce type de problème, une solution consisterait à augmenter le débit CBR, mais cette solution ne convient pas aux cas des applications émettant à un débit constant de 1/T du fait que ces applications avec un nouveau débit offert de 1/T+1/T'=(T+T')/(TT') ne peuvent plus émettre à exactement 1/T. En effet, les cellules OAM introduisent de la gigue.

3.2.1. La solution ATM Forum [AFSEC]

La solution ATM Forum utilise cette approche pour tout échange de messages de sécurité nécessitant de la synchronisation avec le flot de cellules de données utilisateur. Dans la dernière version des spécifications ATM Forum [AFSEC], cette approche sert uniquement au renouvellement des clés de session utilisées pour assurer les services de confidentialité ou d'intégrité des données.

Le renouvellement d'une clé de session s'effectue en deux étapes qui correspondent à l'envoi préliminaire de la nouvelle clé de session et ensuite à l'activation du changement de clé de session. Pour cela deux types de cellules OAM sont définis.

Dans la cellule OAM «d'envoi de la nouvelle clé de session», le transfert de la nouvelle clé de session est protégé par l'application de l'algorithme de renouvellement de clés négocié à l'ouverture de connexion avec la clé maître $K_{m,AB}$ échangée à l'ouverture de connexion (cf. figure 3, l'IE#5).

Une fois l'échange de clé terminé, une cellule «d'activation du changement de clé de session» doit être envoyée pour signaler à l'entité communicante que les données utilisateur qui suivent cette cellule OAM sont chiffrées avec la nouvelle clé. Il est évident que la perte de cette cellule OAM entraînerait la perte de l'ensemble des données. C'est pourquoi, l'ATM Forum envisage d'envoyer plusieurs cellules OAM identiques de suite, et pour éviter la perte de l'ensemble de ces cellules OAM qui pourrait se produire en cas de congestion du réseau, l'ATM Forum propose de les envoyer à intervalles de temps réguliers.

3.3. Négociation au travers d'un canal auxiliaire

La notion de canal auxiliaire s'applique ici lorsque des informations de sécurité sont échangées sous forme de cellules de données utilisateur.

3.3.1. La solution Daniel Stevenson et al. [Ste95]

Stevenson et al. proposent de négocier des clés de session à l'ouverture de connexion non pas dans les messages de signalisation mais comme premières données utilisateur envoyées.

La figure 6 présente cette solution dans le contexte de proxies. Les proxies A et B sont en général placés en coupure sur le réseau par exemple en sortie d'un réseau local pour assurer la protection des communications sur le réseau public ATM.

Comme le montre la figure 6, à l'ouverture de connexion, A envoie sa requête SET UP à son

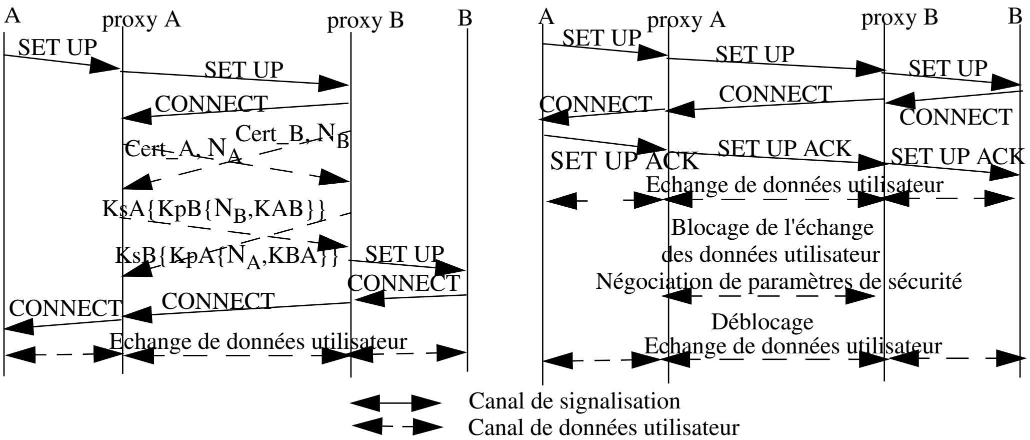

Figure 6 : Négociation de clés de session à l'ouverture de la connexion via un canal auxiliaire Solution de Stevenson et al.

Figure 7 : Négociation de paramètres de sécurité via le canal auxiliaire Solution ATM Forum

proxy qui la transmet au proxy B. Une fois la connexion ouverte entre les proxies, les proxies A et B négocient des clés de session en échangeant tout d'abord leur certificat de clé publique et un nonce, puis un jeton contenant leur clé de session unidirectionnelle chiffrée qui sert également d'authentificateur. Une fois la négociation des clés effectuée, les proxies A et B achèvent alors l'ouverture de connexion entre A et B qui sont alors autorisés à échanger des données utilisateur.

3.3.2. La solution ATM Forum [AFSEC]

Cette solution est utilisée pour négocier des paramètres de sécurité (mécanismes de sécurité, etc.), faire de l'authentification ou échanger des clés, tout comme la solution section 3.1.1.2 le permet. Cependant elle offre l'avantage de ne pas nécessiter de modifications du protocole de signalisation [AFSIG]. Cette solution peut également être utilisée pour effectuer une authentification mutuelle à trois passes à l'ouverture de connexion (si l'authentification à deux passes effectuée dans la signalisation section 1.1.1.1 n'est pas de niveau suffisant) ou bien une authentification en cours de connexion.

Cette solution s'inscrit dans un contexte de proxies, mais contrairement à la solution de Stevenson, l'échange d'informations de sécurité peut s'effectuer au cours de la connexion car les proxies peuvent bloquer les échanges de données entre A et B à tout moment pour négocier de nouveaux paramètres de sécurité comme le montre la figure 7.

3.4. Analyse comparative

Les solutions de Chuang et Deng n'ont pas la même philosophie que celle de l'ATM Forum et Télécom Bretagne en ce sens qu'elles utilisent la signalisation comme support pour négocier des services de sécurité plutôt qu'elles ne protègent les messages de signalisation. Ceci est particulièrement visible par la façon de réaliser le service d'authentification. Pour Chuang et Deng, il fait partie du protocole d'échanges de clés tandis que pour l'ATM Forum (cf. section 3.1.1.1 ou 3.1.1.2) et Télécom Bretagne, il apparaît sous forme d'une signature qui porte sur le message de signalisation et qui garantit ainsi en plus de l'identité de l'émetteur du message, son intégrité. Notons également que pour Chuang et Deng l'authentification n'est envisagée que dans les messages d'ouverture de connexion tandis que les solutions ATM Forum (cf. section 3.1.1.1) et Télécom Bretagne permettent d'authentifier tous les messages de signalisation.

Comme le montre le tableau 3 récapitulant les caractéristiques de chacune des solutions, les solutions ATM Forum et Chuang, respectivement Deng et Télécom Bretagne sont conçues dans des environnements où une ouverture de connexion s'effectue par l'échange de trois, respectivement deux messages de signalisation, ce qui a une grande influence quant au choix des protocoles d'authentification mutuelle et d'échanges de clés à utiliser. Les solutions de l'ATM Forum et de Chuang offrent en effet un plus large choix de protocoles, protocoles à deux ou trois passes. De plus comme les protocoles à trois passes en général à base de nonces sont plus fiables que les protocoles à deux passes à base d'horodateurs (du fait que les horloges sont très difficiles à gérer dans un environnement distribué), les solutions de l'ATM Forum et de Chuang apparaîssent donc comme les solutions les plus fiables. A noter cependant que la solution ATM Forum basée sur une ouverture de connexion en trois messages de signalisation n'est pas conforme aux spécifications [AFSIG] actuelles contrairement aux solutions de Deng et Télécom Bretagne.

Ces solutions peuvent également être comparées en terme de modifications à apporter aux spécifications [AFSIG] (cf. tableau 3). Les solutions de Deng, ATM Forum (sections 3.1.1 et 3.2.1) et Télécom Bretagne nécessitent d'introduire : pour Deng 12 nouveaux IEs, pour l'ATM Forum 7 nouveaux IEs et de nouvelles cellules OAM de sécurité et pour Télécom Bretagne un seul IE de sécurité. Par contre les solutions de Stevenson et Chuang ne requièrent aucune modification de [AFSIG] car les modifications apportées sont transparentes pour le réseau. En effet, Stevenson agit sur le contenu même de la connexion et Chuang modifie au niveau applicatif le traitement des terminaux et serveurs (logiciels).

Il est possible de comparer les solutions suivant le niveau de protection assuré lors de la négociation des services de sécurité. En effet, le fait que les services de sécurité soient négociés dans des IEs qui transitent en clair sur le réseau - IEs#2 à 4 pour Deng, et IEs#1 et 2 pour l'ATM Forum (section 3.1.1.2) - peut affaiblir la sécurité des échanges de données car la seule connaissance des algorithmes de chiffrement utilisés permet de casser plus facilement la clé utilisée. D'autre part, la connaissance des niveaux de confidentialité et d'intégrité (IEs #2 et #6) choisis pour la solution de Deng ou la connaissance du niveau de sensibilité des données à échanger (dans l'IE de contrôle d'accès) pour la solution ATM Forum (section 3.1.1.3) peut également renseigner sur le type de données qui vont être échangées. Pour pallier à ce type de problème, une solution consiste à chiffrer les informations de sécurité, comme le propose Télécom Bretagne.

Toutes ces solutions comportent des inconvénients énumérés ci-après.

Les solutions Deng, ATM Forum (section 3.1.1) et Télécom Bretagne qui définissent de nouveaux IEs nécessitent une totale transparence des équipements du réseau. Or les opérateurs sont assez réticents à l'idée de faire transiter via la signalisation des IEs qu'ils ne connaissent pas et dont ils ne peuvent même pas vérifier le contenu. En effet, rien n'empêche les utilisateurs de faire passer par ces IEs des données utilisateur. De plus, si la signalisation est gratuite, cela signifierait que n'importe qui peut transmettre des informations (de contenu bien entendu limité) sur le réseau gratuitement.

La solution de Chuang s'applique à un environnement spécifique et ne correspond pas à la philosophie ITU ou ATM Forum pour laquelle chaque équipement du réseau participe à la gestion et au contrôle du réseau.

Il est à noter également que la solution de Stevenson ne permet pas la renégociation de paramètres de sécurité au cours d'une connexion contrairement aux solutions de Chuang et ATM Forum (sections 3.2.1 et 3.3.2). Les paramètres ne peuvent être négociés qu'une seule fois à l'ouverture de connexion. Pour les solutions de Deng et Télécom Bretagne, la renégociation au cours d'une connexion est limitée à l'échange de clés de session.

4. L'échange de données

La mise en place des services de sécurité négociés section 3 permet de protéger l'échange de données utilisateur.

Trois approches sont étudiées selon que le service de confidentialité est rendu :

- au niveau de la couche ATM ([Ste95],[Chu96],[AFSEC])
- dans la couche AAL ([Den95])
- au dessus de la couche AAL ([Pau96])

4.1. Confidentialité sur la couche ATM

Le chiffrement est effectué au niveau des cellules ATM, c.à.d. seule la charge utile des cellules est chiffrée. Un problème majeur résulte du chiffrement au niveau de la couche ATM. En effet, suivant les algorithmes de chiffrement utilisés, le niveau de sensibilité aux propagations d'erreurs varie. Une erreur sur un flot de données chiffrées en DES ECB (*Electronic Code Book*), respectivement DES CBC (*Cipher Block Chaining*) implique la perte d'un bloc de 64 bits, respectivement plusieurs blocs de 64 bits, du fait qu'en mode ECB les blocs de données sont chiffrés indépendamment les uns des autres tandis qu'en mode CBC un bloc chiffré est généré à partir du bloc en clair et de tous les blocs précédemment chiffrés. Pour se prémunir de pertes trop lourdes, il est nécessaire de réguliément resynchroniser les dispositifs de chiffrement/déchiffrement. Ceci permet de limiter l'impact d'une erreur sur les données envoyées entre deux cellules de synchronisation. Les solutions suivantes précisent la méthode de synchronisation utilisée.

4.1.1. La solution de Daniel Stevenson et al. [Ste95]

Stevenson et al. définissent une unité cryptographique (encore appelé proxy section 3.3.1) placée en coupure sur le réseau et chargée de chiffrer le trafic cellule par cellule avec une clé de chiffrement par connexion. Ils posent le problème de commuter les clés (*key agility*) suffisamment rapidement pour que les flots de cellules de différentes connexions puissent être chiffrés indépendamment. Ils résolvent également le problème de synchronisation en insérant des informations de synchronisation dans les cellules OAM ou dans des cellules de données de contenu spécifique (mais non précisé dans [Ste95]).

4.1.2. La solution de Shaw-Cheng Chuang [Chu96]

Chuang définit un cryptonode comme un dispositif chargé de chiffrer les données utilisateur sur la couche ATM avec une clé de chiffrement par connexion. Il résout les problèmes de synchronisation au niveau de la couche AAL en insérant des jetons AAL5 PDU qui se distinguent des AAL PDUs de données par un champ de l'AAL5 PDU et par leur longueur qui doit faire 40 octets pour qu'un jeton à transmettre nécessite l'envoi de exactement une cellule ATM. Les jetons AAL5 PDU contiennent les paramètres de sécurité (e.g. numéro de clé) à utiliser pour déchiffrer les cellules ATM de données arrivant directement après ces jetons. Ainsi, à la détection d'un changement de paramètres de sécurité au niveau de la couche AAL (deux jetons consécutifs contiennent des numéros de clés différents par exemple), le cryptonode récepteur doit générer une interruption pour que le déchiffrement mis en place au niveau de la couche ATM s'arrête et soit momentanément contrôlé par la couche AAL pour la mise en place des nouveaux paramètres de sécurité. Le fait que la synchronisation et le chiffrement soient réalisés par des couches du modèle ATM différentes peut provoquer un retard dans l'application des informations de synchronisation sur le déchiffrement des cellules. En effet, il est probable que le jeton arrive mêlé à un flot de cellules de donnée de la même connexion ; or pendant que le jeton est traité au niveau AAL (décapsulation, détection du jeton AAL5 PDU), certaines cellules de données risquent d'être déchiffrées au niveau ATM avec l'ancien contexte de sécurité (e.g. anciennes clés).

En plus de la synchronisation, ces jetons permettent d'assurer les services d'intégrité/authentification en transportant outre le numéro de clé utilisé pour le chiffrement des données, une signature et le numéro de clé utilisé pour générer la signature.

4.1.3. La solution ATM Forum [AFSEC]

L'ATM Forum propose de protéger les échanges de données utilisateur en confidentialité et en intégrité (avec une clé de chiffrement pour chacun de ces services) et optionnellement de détecter tout déséquencement ou rejeu de données. Le service de confidentialité peut être assuré de bout en bout (entre terminaux) ou entre commutateurs tandis que le service d'intégrité n'est assuré que de bout en bout. De ce fait, l'ATM Forum préconise de placer le service de confidentialité au niveau de la couche ATM mais n'exclut pas la possibilité de le placer au niveau de la couche AAL pour un service de confidentialité à rendre de bout en bout.

L'ATM Forum place les services d'intégrité et de détection du déséquencement/rejeu de données au niveau de la couche AAL en ajoutant à l'AAL SDU à protéger une signature portant sur cet AAL SDU, un numéro de séquence et un horodateur. Comme la section 3.2.1 le décrit, les cellules de gestion OAM de sécurité permettent d'assurer la synchronisation des entités de chiffrement/déchiffrement (terminaux ou commutateurs) du point de vue du chiffrement/déchiffrement mais également de la renégociation de clés de session.

4.2. Confidentialité dans la couche AAL

Le chiffrement des données est effectué dans la couche AAL avant leur segmentation en cellules ATM.

4.2.1. La solution Robert H. Deng et al. [Den95]

Deng et al. définissent une couche dédiée à la sécurité à insérer entre deux sous-couches de l'AAL. Cette couche est appelée DPL pour *Data Protection Layer* et chargée d'assurer les services de confidentialité et d'intégrité (avec la même clé de chiffrement pour ces deux services) et optionnellement la détection de déséquencement de données. Le DPL chiffre et signe chaque DPL SDU indépendamment les uns des autres, avec les clés négociées à l'ouverture de connexion section 3.1.2 et les paramètres de sécurité (vecteur initial) contenus dans chaque DPL SDU. Cette solution ne nécessite donc pas d'informations de synchronisation de chiffrement/déchiffrement.

En plus de l'échange de clés de session réalisé à l'ouverture de connexion (cf. section 3.1.2), le DPL peut renouveler les clés de session au cours d'une connexion en bloquant tout échange de données et en envoyant répétivement un DPL PDU contenant la nouvelle clé de session (chiffrée avec sa clé privée) jusqu'à réception d'un acquittement. Cette solution paraît particulièrement gênante pour les connexions de type CBR (*Constant Bit Rate*) et les connexions unidirectionnelles. D'autre part elle ne permet pas d'échange de clés fiable du fait qu'aucun protocole d'authentification fort n'est utilisé.

4.3. Confidentialité au dessus de la couche AAL

Le service de chiffrement est ici effectué au dessus de la couche AAL.

4.3.1. La solution Télécom Bretagne [Pau96]

La solution Télécom Bretagne est proche de la solution de Deng et s'inspire de la norme IEEE 802.10 ([IE802.10A],[IE802.10B]) du fait que tous les services de sécurité protégeant les échanges de données sont rendus sur une couche supplémentaire dédiée à la sécurité. Cette couche est placée au dessus de la couche AAL et est appelée couche SDE (pour *Secure Data Exchange*) en référence à la norme IEEE 802.10.

Comme le montre la figure 8, la couche SDE est chargée d'encapsuler les données utilisateur (SDE SDU) avec deux entêtes, l'un en clair et l'autre chiffré.

Voici les différents services offerts par la couche SDE :

- la confidentialité des données utilisateur. Le champ *SAID* en clair identifie le contexte de sécurité (négocié section 3.1.4) utilisé pour chiffrer les données utilisateur (SDE SDU). Les champs *Padding length* et *Padding* permettent d'aligner les données à chiffrer sur une longueur adéquate dépendant de l'algorithme de chiffrement utilisé.
- l'intégrité/authentification. Le champ *ICV* (*Integrity Control Value*) calculée sur la partie chiffrée du SDE PDU peut servir à authentifier l'émetteur des données et vérifier l'intégrité des données. Cependant, si le service de confidentialité est présent, il est possible de simplifier l'implémentation de ces deux services : le champ *ICV* peut être un simple contrôle CRC (*Cyclic Redundancy Check*) et le service d'authentification peut être rendu en plaçant dans le champ *Negociated number* un numéro secret négocié à l'ouverture de connexion dans l'IE de sécurité (dans *Authentication/integrity Element*).
- le bourrage (cf. annexe 2). Ce service consiste à insérer dans le flux de données utilisateur SDE SPUs des SDE PDUs de contenu non significatif. Ces SDE PDUs sont identifiées par une valeur particulière du *Flag*,
- la détection de déséquencement/rejeu de données utilisateur. Le champ *Sequence number* permet de garantir l'ordre et l'unicité des données utilisateur SDE PDUs.

Tout comme pour la solution de Deng, la synchronisation est réalisée sur chaque SDE PDU en précisant dans chaque SDE PDU dans le champ *User* des informations de synchronisation telles que les numéros de clé à utiliser pour chiffrer ou générer l'*ICV*.

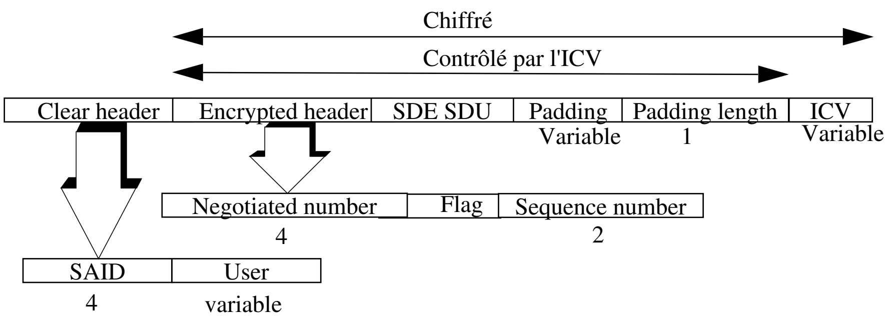

Figure 8 : La construction d'un SDE PDU pour la solution Télécom Bretagne

4.4. Analyse comparative

Comme le montre le tableau 2, les solutions diffèrent en terme de services de sécurité rendus. Stevenson se limite au seul service de confidentialité tandis que l'ATM Forum, Chuang et Télécom Bretagne implémentent en plus le service d'intégrité avec pour l'ATM Forum en option le service de prévention contre le déséquencement/rejeu et pour Télécom Bretagne les services de bourrage et de prévention contre le déséquencement/rejeu de données. Pour ces solutions, le service d'intégrité est rendu au niveau AAL ou au dessus soit en ajoutant une signature aux AAL SDUs ou SDE SDUs de données (ATM Forum, Télécom Bretagne) soit en intégrant dans un jeton AAL5 PDU une signature (Chuang). Comme le souligne Chuang dans [Chu96], la solution de définir un AAL SDU spécifique à la sécurité est préférable à celle de l'ATM Forum car l'introduction d'une signature dans un AAL SDU de données risque d'accroître la taille de l'AAL SDU au delà des limites fixées par la couche AAL, ce qui obligerait à faire une nouvelle fragmentation et réduirait les performances.

Pour toutes les solutions présentées exceptée celle de Stevenson, le service d'intégrité est toujours rendu au niveau de la couche AAL ou au dessus pour éviter des segmentations supplémentaires de cellules. Par contre le service de confidentialité est placé soit sur la couche ATM soit au dessus (dans ou au dessus de l'AAL).

Placer le service de confidentialité sur la couche ATM possède les avantages de simplifier le traitement du chiffrement qui porte sur des blocs de taille fixe de 48 octets et de permettre des vitesses de chiffrement importantes du fait de son intégration dans le hardware. Cependant cela réduit le choix des algorithmes de chiffrement possibles.

Placer le service de chiffrement au sein de la couche AAL (avant la segmentation) ou au dessus a aussi des avantages. Les modifications à apporter au modèle non sécurisé sont limitées à une seule couche (la couche AAL pour Deng et la couche SDE pour Télécom Bretagne). Le problème du *key agile* est réduit puisque les données sont chiffrées par blocs de longueur importante (jusqu'à 65535 octets pour le DPL SDU). Pour les solutions préconisées par Deng et Télécom Bretagne, les blocs DPL SDUs et SDE SDUs sont chiffrés indépendamment les uns des autres ; la synchronisation pour le chiffrement/déchiffrement s'effectue donc naturellement. En fait, pour Deng, seul le changement de clés de session nécessite d'être synchronisé avec le flot de données utilisateur et pour cette solution, la synchronisation est plus simple à mettre en place que dans la solution de Chuang (cf. section 4.1.2) car elle s'effectue dans la même couche que le chiffrement, tout comme pour la solution ATM Forum.

Par contre, placer le service de chiffrement sur ou au dessus de la couche AAL est moins fiable que sur la couche ATM car les en têtes des couches DPL PDU, SDE PDU, AAL PDU restent en clair.

Il est à noter que contrairement aux solutions de Chuang, ATM Forum et Télécom Bretagne, la solution de Deng ne permet pas une totale indépendance entre services de confidentialité et d'intégrité (cf. tableau 3). En effet une seule clé de session est définie pour ces deux services, ce qui limite le choix des mécanismes à utiliser et affaiblit les services de sécurité. En effet si un intrus parvient à casser la clé de session, il peut non seulement déchiffrer les données envoyées dans une direction (clé unidirectionnelle) mais en générer et les signer. De plus, si l'échange de clés de session est uniquement protégé par le chiffrement avec la clé de session, l'intrus peut récupérer la nouvelle clé de session utilisée.

a	Stevenson et al.	Deng et al.	Chuang	ATM Forum	Télécom Bretagne
services de sécurité mis en place via le flux de signalisation		A, EC, PR, NS:I+C	A, EC, PR, NS:I+C+EC	A, I, CA, EC, PR NS:I+C+EC+A et ce pour tous les messages de signalisation	(A, I, C, PR, NS:C+I+A+B+PR) et ce pour tous les messages de signalisation
services de sécurité mis en place via le flux de gestion				EC	
services de sécurité mis en place via le canal auxiliaire	EC, A, PR			NS, A, EC	
services appliqués aux données utilisateur	C sur ATM S par cellules OAM ou cellules de données utilisateur de contenu connu	C, I, et (PR) sur AAL S sur chaque DPL-PDU EC par un DPL-PDU	C sur ATM I, A sur AAL S sur AAL par un jeton AAL5 PDU	C plutôt sur ATM I, A et (PR) sur AAL S par cellules OAM	(C, I, A, PR, B) au dessus de AAL S sur chaque SDE PDU

Tableau 2 : Récapitulation des services de sécurité offerts par les solutions de sécurité ATM

a. Notations utilisées :

A Authentification
B Bourrage
C Confidentialité
CA Contrôle d'accès
EC Echange de Clés
(XX) Service XX optionnel
I Intégrité
NS:XX Négociation du service de sécurité XX
PR Prévention contre le Rejeu
S Synchronisation

	Stevenson et al.	Deng et al.	Chuang	ATM Forum	Télécom Bretagne
renégociation des paramètres de sécurité	non	oui, échange de clés de session par le biais des DPL-PDU	oui, via la signalisation	par le biais du flux de gestion ou de la connexion auxiliaire	échange de clés par le biais d'une connexion auxiliare
protocole d'authentification et/ou de négociation de clés	basé sur des algorithmes asymétriques	X509 à deux passes	protocoles à deux ou trois passes	dans le flux de signalisation avec des protocoles à deux ou trois passes	protocoles à deux passes
modifications à apporter aux spécifications [AFSIG]	aucune (sauf si la synchronisation se fait via des cellules OAM de sécurité)	définition de 12 nouveaux IEs	aucune - modifications logiciels uniquement	définition de 7 nouveaux IEs et de nouvelles cellules OAM de sécurité	définition d'un nouvel IE
séparation nette entre services de confidentialité et d'intégrité		non	oui	oui	oui

Tableau 3 : Récapitulation des solutions de sécurité ATM

5. Conclusions

Dans cet article, nous présentons et comparons les solutions proposées par Stevenson et al., Deng et al., ATM Forum, Chuang et Télécom Bretagne pour assurer la sécurité des communications sur les réseaux ATM.

Ainsi contrairement à la solution ATM Forum qui vise à satisfaire à la fois les problèmes des opérateurs et des utilisateurs, les solutions de Stevenson, Chuang, Deng et Télécom Bretagne sont plutôt orientées utilisateurs, c.à.d elles cherchent à assurer la sécurité des communications de bout en bout, d'utilisateur à utilisateur au travers du réseau public.

La solution proposée par Chuang est inexploitable dans un environnement ATM standard du fait qu'elle est liée à une architecture spécifique.

Du fait que la solution ATM Forum est toujours en cours de spécifications (la version 5 des spécifications sur la sécurité est sortie en octobre 1996), elle reste pour l'instant imprécise et parfois incohérente. D'autre part, avec la nouvelle direction prise par les travaux de l'ATM Forum, à savoir la possibilité d'une ouverture de connexion à trois échanges de messages de signalisation, elle se place en non conformité avec les spécifications ATM Forum sur la signalisation [AFSIG].

Les solutions ATM Forum et Télécom Bretagne sont sans aucun doute les solutions les plus complètes en termes de services de sécurité rendus, nombre de paramètres négociables, niveau de détail de la réalisation (structure de messages).

La solution Télécom Bretagne est la seule solution à proposer d'assurer la confidentialité d'une partie de la signalisation (cf. tableau 2). Avec ce service, contrairement aux solutions de Deng, Chuang et ATM Forum, il est possible d'effectuer la négociation de services de sécurité via la signalisation tout en préservant la confidentialité des paramètres de sécurité échangés. Ce service peut également permettre à des réseaux locaux interconnectés de maintenir leur plan d'adressage secret.

La solution ATM Forum est la solution qui offre le plus grand choix quant à la méthode utilisée pour négocier ou renégocier les services de sécurité, mais c'est aussi la solution la plus compliquée à implémenter. D'ailleurs à ce jour, seules les solutions de Chuang et Télécom Bretagne sont implémentées. Pour la solution Télécom Bretagne, en fait, seule la partie relative à la négociation de services de sécurité est implémentée.

6. Références

[AFSEC] ATM Forum, «ATM Forum 95-1473R5, Phase I ATM security specification», octobre 1996.

[AFSIG] ATM Forum, «ATM User-Network Interface Specification», version 3.1, 1994.

[Chu96] Shaw-Cheng Chuang, «Securing ATM networks», Third ACM conference on computer and communication security, New Delhi, Inde, mars 1996.

[Cros95] S.A. Crosby, «Performance management in ATM networks», thèse, University of Cambridge, mai 1995.

[Den95] Robert H. Deng, Li Gong and Aurel A. Lazar, «Securing data transfer in Asynchronous Transfer Mode networks», Proceedings of Globecom'95, Singapour, pp. 1198-1202, novembre 1995.

[I321] CCITT I.321, «B-ISDN Protocol Reference Model and its applications», 1991.

[IE802.10A] IEEE 802.10, «Standard for Interoperable LAN security (SILS) - Part A: The Model», décembre 1989.

[IE802.10B] IEEE 802.10 «Standard for Interoperable LAN Security (SILS) - Part B: Secure Data Exchange», janvier 1990.

[Lau95] Maryline Laurent, Pierre Rolin, «Sécurité ATM : une analyse de flux menée sur quatre architectures de réseaux», GRES'95, Paris, septembre 1995.

[Lau96] Maryline Laurent, «Sécurité ATM : analyse de la sécurité des échanges sur l'architecture du LAN Emulé», CFIP96, Rabat, Maroc, octobre 1996.

[Pau96] Olivier Paul, «Conception et implémentation d'un module de sécurité pour les réseaux ATM», Rapport ME-96001, Télécom Bretagne, septembre 1996.

[Pry91] Martin de Prycker, «Asynchronous Transfert Mode: Solution for broadband ISDN», Ellis Horwood, New York, 1991.

[Q2963] ITU-T I.311, «B-ISDN. Digital Subscriber Siignaling System No2 (DSS2) connection modification - Peak Cell Rate modification by the connection owner», novembre 1995.

[Ste95] Daniel Stevenson, Nathan Hillery ans Greg Byrd, «Secure Communications in ATM Networks», Communications of the ACM, Vol. 38, No. 2, février 1995.

[X800] UIT-T X.800, «Réseaux de communication de données: interconnexion de systèmes ouverts (OSI); sécurité, structure et applications. Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT», 1991.

Annexe 1 : Acronymes

AAL: ATM Adaptation Layer
DPL: Data Protection Layer
IE: Information Element
OAM: Operation And Maintenance
PDU: Protocol Data Unit
SAID: Secure Association Identifier
SDE: Secure Data Exchange
SDU: Service Data Unit

Annexe 2 : Les services de sécurité

- authentification de l'origine des données : "Confirmation que la source des données reçues est telle que déclarée" [X800]. Ce service consiste en général à adjoindre aux données, une signature digitale calculée sur ces données à l'aide d'une fonction de hashing, un algorithme de chiffrement et une information secrète (**clé**). La signature permet de garantir l'identité de l'émetteur des données du fait que seul le possesseur de la bonne information secrète a pu générer cette signature. Elle permet également de garantir l'intégrité de ces données.

- bourrage : "Production d'instances de communication parasites, d'unités de données parasites et/ou de données parasites dans des unités de données" [X.800]. Ce service consiste à générer du trafic supplémentaire de contenu non significatif sur une connexion de telle sorte que par l'analyse du trafic échangé sur cette connexion, aucune information ne puisse être déduite sur la quantité réelle de données échangées, la fréquence des échanges, etc. Bien entendu, ce service suppose que le service de confidentialité soit rendu.

- confidentialité : "Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés" [X800]. Ce service consiste à chiffrer des données, c'est à dire à brouiller de façon pseudo-aléatoire ces données à l'aide d'une information secrète (clé) de telle sorte que seul le détenteur de la bonne information secrète est capable de déchiffrer ces données et de retrouver leur contenu originel. En général, cette information secrète est une **clé**. Afin d'assurer un service de confidentialité fiable protègeant les échanges de données sur une connexion, il est nécessaire que les deux entités communicantes conviennent régulièrement de nouvelles clés. Les différentes clés utilisées au cours d'une connexion sont appelées **clés de session**.

- contrôle d'accès : "Précaution prise contre l'utilisation non autorisée d'une ressource ; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée" [X800].

- intégrité des données : "Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée" [X800].