Institut Eurécom
2229, Route des Crêtes
BP 193
06904 Sophia Antipolis CEDEX
FRANCE

Research Report 92-000

Protocoles d'Authentification dans le Réseau Intelligent

Contribution au premier rapport semestriel du projet Ernestine II

Refik Molva

31/08/1992

Refik Molva
E-mail: molva@eurecom.fr
Tel: (+33) 93 00 26 12

Résumé

Ce papier propose une conception du service d'authentification pour les réseaux intelligents. Deux nouveaux Service Independent building Blocks (SIB) sont introduits pour permettre l'utilisation des mécanismes d'authentification dans le plan fonctionnel global. Une suite de protocoles définissent les échanges de messages cryptographiques pour différents schémas d'authentification possibles. La relation entre les SIB d'authentification et leur réalisation par des entités fonctionnelles distribuées qui implémentent le protocole est aussi présentée assez brièvement.

1. Les besoins d'authentification dans les services du R.I.

Les besoins pour des mécanismes d'identification et de contrôle d'accès sont particuli\erement importants dans le cas des services à valeur ajoutée qui ne sont pas basés sur des mécanismes de protection physiques. Pour ce type de services, l'absence d'un point de raccordement physique par lequel les utilisateurs peuvent être identifiés est la raison principale pour laquelle une fonction d'identification logique appelée **authentification** est nécessaire. Ce terme désigne tout procédé qui permet à une entité du réseau de prouver son identité à une entité distante en échangeant des messages à caractère spécial.

L'enjeu sur le développement des techniques d'authentification qui permettront l'identification des utilisateurs en l'absence d'une identification basée sur le raccordement physique est d'autant plus grand que le succès de la plupart des services du réseau intelligents dépendra directement de leur niveau d'intégrité .

Le besoin d'authentification apparaît à deux niveaux distincts:

- l'authentification de l'utilisateur (l'abonné) par le fournisseur du service: cette fonction est nécessaire pour le contrôle d'accès au service à la valeur ajoutée. Ce type d'authentification permet au fournisseur du service de s'assurer que seuls les utilisateurs autorisés (ceux qui sont couverts par le facturation) accèdent au service. De ce fait, un mécanisme d'authentification unidirectionnelle serait suffisant pour répondre à ce besoin, dans le sens que seul l'identification de l'utilisateur par le service est nécessaire et que l'authentification dans le sens inverse n'est pas strictement impliqué.

- l'authentification bout en bout: dans le cas où le service permet à deux entites de se communiquer entre elles, l'authentification de ces entités, l'une par l'autre, réciproquement ou seulement dans un sens peut être nécessaire. Si ces entités font confiance au service dans la mesure où chacune aura été authentifiée par le service et que la corroboration de l'identité de l'interlocuteur par le service est estimée suffisante par chaque entité, la fonction précédente est suffisante pour répondre au besoin d'authentification

bout en bout. Par contre, si les entités communicantes ne font pas confiance au réseau, il est nécessaire de fournir une fonction supplémentaire pour répondre au besoin d'authentification bout en bout.

Ces besoins d'authentification sont très apparents pour le service Universal Personal Telecommunications (UPT) permettant à un abonné de pouvoir déplacer son numéro d'abonné et son point d'accès au réseau à n'importe quel point du globe et le service Virtual Private Network (VPN) permettant de réaliser un réseau privé (un plan de numérotation) d'une manière logique et sans allocation de circuits spécialisés. Dans les deux cas, les abonnés accèderont aux services sans pouvoir bénéficier de protection physique, c.-à-d., en utilisant des terminaux publics et des lignes comutées (non spécialisées) vulnérables à toute forme d'intrusion et d'imposture, d'où découlent les besoin d'authentification de ces services.

2. Le service d'authentification dans le GFP

Il existe deux alternatives concernant la définition du service d'authentification dans le plan GFP (Global Functional Plane):

1) La fonction d'authentification spécifique à un service peut être représentée par un schéma logique (GSL) en utilisant des SIB (Service Independent building Block) existant comme les SIB Verify, Compare, User Interface et quelques autres SIB élémentaires qui seraient définis pour permettre l'introduction des traitements relatifs à la sécurité, comme le cryptage-décryptage, etc.

2) Un ou quelques SIB spécifiques à l'authentification peuvent être définis.

Nous avons choisi la deuxième alternative car bien que la première permette la définition de mécanismes d'authentification spécifiques à chaque service, une étude préalable a montré d'une part que la fonction d'authentification est bien indépendante de la nature du service englobant, et d'autre part, que le fait d'introduire des SIB spécifiques pour l'authentification permet de définir d'une manière permanente les mécanismes de plus bas niveau (plan DFP et plan physique) implémentant la fonction d'authentification. Grâce à ce dernier point la description des mécanismes d'authentification, tâche qui souvent nécessite une expertise bien particulière, sera épargnée au concepteur d'un nouveau service utilisant l'authentification permettant ainsi d'éviter l'introduction d'erreurs de conception dans le domaine de la sécurité.

Le service d'authentification sera défini par deux SIB: le SIB Sign-on et le SIB peer-authentication.

Le SIB Sign-on réalise l'authentification initiale d'un abonné par le réseau et permet à l'abonné d'obtenir des preuves de son authentification qui peuvent être utilisées pendant l'authentification point-à-point si cette dernière a lieu.

Le SIB peer-authentication met en Ïuvre l'authentification point à point entre deux entités. L'authentification point à point est nécessaire si l'une ou l'autre des entités qui y participent ne font pas confiance à l'authentification effectuée par le réseau (le Sign-on) et veulent effectuer elles-mêmes la vérification de leur partenaire. Les entités concernées peuvent être deux abonnés ou des applications représentant deux abonnés, un abonné et un serveur d'application faisant partie du réseau.

La représentation de ces fonctions en deux SIB séparés est justifiée par le fait que les deux fonctions ne sont pas nécessairement invoquées simultanément ni avec la même fréquence d'utilisation.

2.1. Le SIB Sign-on

Le SIB Sign-on est invoqué à l'initiation d'un appel pour identifier un abonné en utilisant des procédures d'authentification forte. A l'issue de cette opération, si l'abonné a été authentifié avec succès, le terminal de l'abonné est muni de certificats cryptographiques qui lui permettront d'entreprendre, si le service le requiert, une ou plusieurs sessions d'authentification point à point (peer authentification) et de distribution de clés secrètes.

Les interfaces du SIB Sign-on sont décrites dans le schéma de la figure 1.

Figure 1: Le SIB Sign-on

La signification des termes utilisés dans ce schéma est la suivante:

termes définissant les paramètres spécifiques au service :

- **type de protocole:** comme plusieurs variantes des protocoles peuvent exister dans le réseau, ce terme désigne le type de protocole qui doit être utilisé dans le cas du service courant. Les différents types de protocoles peuvent se distinguer par le choix de l'algorithme cryptographique (à clé publique, conventionnel, etc.), mais il peut également y avoir de protocoles différents au sein d'une même famille cryptographique suivant les besoins d'un service

particulier (authentification dans un sens de l'abonné vers le réseau, authentification mutuelle, etc.).

termes définissant les paramètres spécifiques à chaque appel:

- **caractéristiques du terminal:** ce terme désigne les fonctions d'authentification fournies par le terminal par lequel l'abonné effectue son authentification. Ces fonctions peuvent consister en un simple clavier numérique, une calculette pouvant effectuer des calculs cryptographiques, un lecteur de carte à puce ou un terminal de donnée.
- **compte-rendu d'authentification:** c'est le résultat de l'opération d'authentification, y compris la raison pour laquelle l'authentification a échoué si c'était le cas.

Il est important de noter qu'aucun des deux SIB liés à l'authentification ne fournit des éléments de preuve comme des certificats de clés ou des authentificateurs (certificats d'identité). Ce type de données est échangé entre les éléments distribués et sera visible dans la spécification distribuée des SIB (plan DFP).

2.2. Le SIB Peer Authentication

Ce SIB représente la fonction d'authentification point à point entre l'abonné appelant qui a effectué son "Sign-on" et l'abonné appelé ou une entité interne du réseau ou du service. A l'issue de cette authentification l'abonné et l'entité destinataire sont mutuellement assurés de leur identité, en plus le terminal de l'abonné et celui de son partenaire d'authentification possèdent une clé secrète qui peut être utilisée pour effectuer d'autres opérations en vue d'assurer la confidentialité et l'intégrité des messages échangés.

Figure 2: Le SIB Peer Authentication

La signification des paramètres d'interfaces du SIB Peer Authentication est identique à celle des paramètres du SIB Sign-on, à l'exception du paramètre supplémentaire qui indique les caractéristiques du destinataire dans le cas d'une authentification point à point. Ce paramètre indique si le destinataire est un abonné ou une entité interne du réseau ou du service et dans le cas où c'est un abonné les fonctions d'authentification supportées par le terminal de l'abonné sont précisées par ce paramètre.

Les mécanismes correspondants au SIB Sign-on et au SIB Peer Authentication seront définis par les interactions entre les éléments fonctionnels distribués du plan DFP. Mais avant d'aborder la description spécifique à ce plan, nous allons d'abord présenter les protocoles d'authentification qui définissent l'échange des messages de sécurité entre les différents acteurs des procédures d'authentification.

3. Les protocoles d'authentification

Nous définissons tout d'abord les entités qui sont impliquées dans les procédures d'authentification et leurs fonctions respectives:

- **l'abonné:** l'abonné est impliqué dans toute instance de protocole d'authentification. Les fonctions qui sont exécutées par l'abonné dépendent très fortement des caractéristiques du terminal utilisé pour l'appel. Les cas suivants seront considérés:

  - appareil de téléphone ordinaire avec clavier numérique: dans ce cas la seule fonction d'authentification que peut exécuter l'abonné est l'entrée d'un chiffre correspondant à un PIN. Il ne peut pas générer ni vérifier des messages cryptographiques. Comme elles nécessitent l'entrée et la transmission en texte clair du PIN secret, les procédures d'authentification basées sur ce type de terminal sont intrinsèquement vulnérables aux attaques multiples pouvant provenir du terminal (cheval de Troie) ou de l'écoute sur les lignes.

  - terminal de données: quand l'abonné accède au réseau à travers un ordinateur connecté par une interface de donnée (ISDN), il peut exécuter un protocole plus sophistiqué et plus sûr que précédemment en utilisant des programmes et interfaces de l'ordinateur qui permettent d'effectuer des calculs cryptographiques et d'échanger des messages relativement longs. Si le terminal est l'ordinateur personnel de l'abonné, des clés secrètes l'identifiant peuvent y être stockées et la sécurité du protocole global peut être très bonne. Si le terminal est un ordinateur public, comme l'utilisateur ne peut y stocker ses secrets, il doit les rentrer en texte clair dans l'ordinateur avant qu'ils soient transmis (en clair ou cryptés) et c'est à ce niveau que cette méthode reste vulnérable à des attaques du type cheval de Troie ou à des attaques visant à découvrir le secret de l'utilisateur par des recherches exhaustives en partant des données cryptées observées sur la ligne.

- téléphone ordinaire ou terminal de données avec un dispositif de calcul personnel non-connecté au terminal: il s'agit d'un appareil de calcul avec affichage LCD avec ou sans clavier incorporé et pouvant effectuer des opérations cryptographiques d'après une logique prédéfinie. Cet appareil peut ainsi combler le manque de capacité de calcul chez l'homme. La logique d'authentification qui gère le fonctionnement de ce dispositif nécessite très souvent l'authentification de l'utilisateur par le dispositif lui-même avant de fournir des éléments identifiant l'abonné. La sécurité de ce type d'accès est due au fait que les secrets de l'abonné ne sont livrés à aucun terminal public en évitant ainsi les fuites qui peuvent être occasionnées par les chevaux de Troie et les espions sur les liaisons. Néanmoins le dispositif lui-même ne garantit pas une sécurité absolue et si le de protocole n'est pas bien conçu, il peut y avoir des points de vulnérabilité permettant d'impersonnifier un abonné légitime. D'autre part il existe un désavantage pratique dans ce type de méthode d'identification qui est dû à la nécessité pour l'utilisateur de copier des nombres assez grands entre le dispositif de calcul et le téléphone ou l'ordinateur public.[1]

- téléphone ordinaire ou terminal de données avec un lecteur de carte à puce: c'est de loin la technique la plus sûre et la plus pratique car elle présente tous les avantages des précédentes sans leurs inconvénients. Une fois que l'abonné est authentifié par la carte à puce en utilisant le secret de l'abonné (PIN) par un échange local et non-exposé aux attaques, la carte peut exécuter des opérations aussi complexes qu'il est nécessaire pour atteindre le degré de sécurité désiré afin d'effectuer une authentification au nom de l'abonné à travers les lignes du réseau. Cependant l'inconvénient majeur de cette méthode par rapport à la précédente est le besoin d'équiper le terminal avec un lecteur de carte à puce.

- **le serveur d'authentification (SA):** c'est l'entité centrale qui détient les informations permettant de vérifier l'identité des abonnés et des autres entités qui peuvent être soumises à l'authentification. Ces informations peuvent être constituées, pour chaque entité à authentifier et en fonction de la méthode applicable, de la clé secrète, du PIN ou du mot de passe crypté ou du certificat

[1] Dans le cas d'un poste téléphonique, on peut envisager d'équiper le dispositif de calcul considéré d'un petit haut-parleur émettant des tonalités DTMF. Il suffirait à l'utilisateur d'appliquer ce haut parleur sur le micro du psote téléphonique pour éviter la démarche fastidieuse consistant à recopier un long nombre sur le clavier.

de la clé publique associée à l'entité. Le SA est la seule composante du système qui doit être protégée car la validité de toutes les opérations d'authentification (et de sécurité en général) dépendent du bon fonctionnement et de l'intégrité du serveur. De ce point de vue le SA constitue le talon d'Achille du système. Cependant en ayant concentré toute fonction critique dans le SA, il suffit d'assurer parfaitement sa protection, voire sa protection physique par une isolation du matériel le contenant, pour obtenir une *assurance parfaite* de la *sécurité globale du système* car les protocoles sont conçus pour être robustes en présence de toute forme d'attaque ou d'intrusion pouvant provenir des éléments autres que le serveur.

- **partenaire d'authentification:** c'est l'entité qui est le répondant de l'abonné dans le cas d'une authentification point à point (*peer authentication*). Le partenaire peut être l'abonné appelé ou une entité interne du réseau ou du service comme une application protégée.

Pour chaque SIB il existe un ensemble de protocoles qui peuvent être appliqués dans des situations différentes en fonction des paramètres spécifiques d'un service et d'un appel particulier.

Comme la description des protocoles d'authentification est basée sur l'utilisation des termes cryptographiques, pour la suite de ce rapport nous allons définir la notation suivante:

Notation:

E(k, m) : résultat du cryptage du message m en utilisant la clé k

où **k** désigne :

K_a : la clé secrète de l'entité A avec un algorithme symétrique comme D.E.S. ou avec un algorithme à clé publique comme R.S.A.

K_a' : la clé publique de l'entité A avec un algorithme à clé publique

3.1. Authentification initiale (sign-on)

Les flux de messages suivant présente une vue condensée des différentes versions du protocole d'authentification initiale. La signification des différents champs des messages varie donc d'après la version du protocole.

Abonné SA

jeton_appelant, id_appelant, certificat_appelant, id_service, id_appelé

---------->

jeton_SA , certificat_SA, ticket_appelant, ticket_appelé

<----------

Dans le premier message, l'abonné appelant demande d'être authentifié par le SA. Ce message contient principalement l'identification de l'abonné appelant (**id_appelant**) et un jeton prouvant l'identité de l'abonné appelant (**jeton_appelant**). Ce jeton peut avoir une des formes suivantes d'après la configuration du terminal abonné et d'après le type de protocole:

- **jeton_appelant** = PIN ou mot de passe en texte clair, si le terminal est un téléphone ordinaire.
- **jeton_appelant** = $E(K_{appelant}, temps)$, si le terminal de l'abonné appelant présente d'autres caractéristiques qu'un téléphone ordinaire. Dans ce cas, le cryptage est effectué dans le dispositif de calcul personnel, dans l'ordinateur personnel ou dans la carte à puce. La clé $K_{appelant}$ peut également être choisie comme un nombre aléatoire ou comme étant le résultat d'un calcul qui lui associe une signification particulière comme dans l'exemple suivant:

$$\mathbf{K_{appelant} = E(K_{service}, h(id\_appelant, attributs\_appelant))}$$

où

$K_{service}$ est une clé secrète connue seulement par SA (et éventuellement l'administrateur du service) et associée au service auquel l'abonné appelant veut accéder,

h est une fonction de "hash" qui produit une suite de n bits représentant les paramètres d'entrée, n étant la taille d'un bloc de cryptage et la taille des paramètres d'entrée étant souvent beaucoup plus grande que n,

attributs_appelant représente des attributs spécifiques de l'abonné en ce qui concerne ses droits, la validité de ses privilèges, etc.

Si la clé $K_{appelant}$ est calculée par une fonction comme dans l'exemple ci-dessus, le fait que l'abonné envoie un message crypté par cette clé prouve non seulement son identité mais en plus *l'authenticité de ses attributs*, ce qui permet d'effectuer des contrôles au-delà de l'authentification comme *le contrôle d'accès*

pour les ressources du réseau ou du service. D'autre part, le calcul de E($K_{appelant}$, temps) peut être effectué de plusieurs manières différentes en fonctions du type de terminal et des propriétés des dispositifs utilisés. En règle générale, il est nécessaire que le terminal ou le dispositif (carte à puce ou carte non connectée) qui possède la clé $K_{appelant}$ ne délivre pas l'expression E($K_{appelant}$, temps) avant que l'abonné soit identifié localement . Il existe aussi une solution dans laquelle la clé $K_{appelant}$ n'est pas connue par le terminal ou le dispositif et l'expression envoyée au SA est la combinaison d'un nombre secret calculé par le terminal et du PIN secret de l'utilisateur [1].

Le premier message du protocole contient en outre des éléments optionnels ou qui dépendent de la version du protocole:

- **id_appelé** est l'identificateur de l'abonné appelé ou de l'entité interne au service qui jouera le rôle du partenaire d'authentification point à point, si cette dernière a lieu, la connaissance de cet identificateur par le SA est nécessaire dans le cas où le protocole point à point requiert la distribution d'une clé secrète partagée ou de certificats de clés publiques aux deux entités qui effectueront l'authentification point à point.

- **id_service** est l'identificateur du service appelé qui est présent dans le cas où les fonctions d'authentification sont spécifiques à chaque service; dans ce cas, le SA a besoin de connaître la valeur de ce paramètre pour pouvoir déterminer la fonction de vérification à utiliser (la clé cryptographique globale du service, représentée par $K_{service}$ dans l'exemple ci-dessus).

- **certificat_appelant** est un message signé par SA (ou par l'autorité qui délivre des clés publiques, si celle-ci est distincte de SA) et qui prouve l'intégrité de la clé publique de l'appelé; le certificat de la clé publique K'_a appartenant à l'entité A peut être défini par l'expression suivante:

$$E(K_{SA}, K'_a, A, \text{validité\_temporelle})$$

où E désigne le cryptage par un algorithme à clé publique. Ce type de certificat est utilisé par les entités qui veulent utiliser la clé publique de l'entité A, afin de s'assurer que la clé qui leur est fournie (par l'entité elle-même ou par un service de distribution) est bien celle de l'entité A. Pour ce faire ces entités-là doivent décrypter le certificat en utilisant la clé publique K'_{SA} de SA qui est connue par toutes les entités du système et comparer le résultat du décryptage aux valeurs attendues qui sont la clé qui leur a été fournie et l'identificateur de

l'entité destinatrice. Le champ certificat_appelant n'est présent dans le premier message du protocole que si un algorithme à clé publique est utilisé.

Le deuxième message du protocole est optionnel et n'est échangé que si l'une des conditions suivantes est requise:

- Le terminal de l'appelant est autre qu'un téléphone ordinaire et le protocole nécessite l'authentification mutuelle de l'abonné par le SA et du SA par l'abonné. Dans ce cas le champ **jeton_SA** qui prouve que l'appelant est bien en communication avec le SA (et non pas avec un imposteur utilisant un cheval de Troie) est présent dans le message. Ce champ est de la forme suivante:

  $E(K_{appelant}, f(temps))$ (avec la cryptographie symétrique)

  ou

  $E(K_{SA}, f(temps))$ (avec la cryptographie asymétrique)

  où f est une fonction très simple dont la présence est nécessaire pour produire un résultat différent de l'expression jeton_appelant. Dans le cas où ce champ existe et quand la cryptographie à clé publique est utilisée, le champ **certificat_SA** peut aussi être présent afin de permettre à l'appelant de retrouver la clé publique de SA qui est nécessaire pour la vérification du champ jeton_SA. Si SA et l'autorité qui délivre les clés publiques sont confondues alors le champ certificat_SA peut être omis car la clé publique de SA est connue de toutes les entités par définition.

- si un protocole d'authentification point à point ou un canal secret basé sur la cryptographie symétrique seront invoqués à la suite de l'authentification initiale, les champs **ticket_appelant** et **ticket_appelé** sont présents dans le deuxième message du protocole d'authentification initiale. Ces deux champs permettent au SA de distribuer à l'appelant et à l'appelé une clé secrète K qu'il vient de créer. Le contenu de ces deux champs peut être représenté par les expressions suivantes:

  ticket_appelant = $E(K_{appelant}, K, id\_appelé, validité\ temporelle)$

  ticket_appelé = $E(K_{appelé}, K, id\_appelant, validité\ temporelle)$

3.2. Authentification point à point (peer authentication)

Etant donné l'hypothèse qu'aucune composante du réseau autre que le SA ne peut être fiable du point de vue de la sécurité, le protocole d'authentification point à point doit être exécuté seulement et directement par les entités qui ont besoin de cette authentification.

Dans le cas où ces entités sont toutes les deux des abonnés du réseau, le protocole est entièrement exécuté en dehors du réseau par ces entités elles-mêmes et la description ci-dessous ne peut que servir de recommandation pour la manière dont sera conçu ce protocole. Par contre, si l'entité appelée est une composante interne du service, par exemple un serveur d'application, alors cette entité doit implémenter le protocole ci-dessus et l'abonné appelant (son terminal) doit se conformer à ce protocole.

D'autre part le protocole point à point ne peut être exécuté que si les terminaux des abonnés qui y sont impliqués sont des terminaux autres que le téléphone ordinaire.

En fonction du type de combinaison entre la phase d'authentification initiale et celle d'authentification point à point, il peut exister deux configurations différentes pour le protocole point à point:

- **en mode direct:** les partenaires de l'authentification point à point communiquent directement. Dans ce cas l'authentification point à point a lieu après l'authentification initiale. Ce mode est avantageux dans le cas où plusieurs authentifications point à point doivent avoir lieu après une même authentification initiale.
- **en mode relais:** les partenaires de l'authentification point à point communiquent à travers le SA qui a la charge de vérifier l'identité d'une entité et de traduire le jeton qui identifie cette entité dans un format qui peut être vérifié par la deuxième entité avant de l'envoyer à cette dernière. Dans ce cas le premier message de l'authentification point à point est confondu avec le premier message de l'authentification initiale. Ce mode semble être plus économique en nombre de messages si l'on considère que le nombre et la trajectoire des messages d'authentification dans ce mode est très proche de ceux des messages de signalisation habituels tout en supposant la possibilité de transporter les messages d'authentification dans les mêmes paquets que les messages de signalisation habituels.

3.2.1. Mode direct

Le schéma ci-dessous représente les messages échangés dans le cadre du protocole point à point en mode direct utilisant la cryptographie à clé publique:

Appelant Appelé

$E(K_{appelant}, temps)$, certificat_appelant, id_appelant

---------->

$E(K_{appelé}, temps)$, certificat_appelé, id_appelé

<----------

Le schéma ci-dessous représente le protocole en mode direct correspondant à l'utilisation de la cryptographie symétrique:

Appelant Appelé

E(K, temps), ticket_appelé, id_appelant

---------->

E(K, f(temps)),

<----------

où K désigne la clé partagée distribuée dans ticket_appelant et ticket_appelé (voir le protocole d'authentification initiale).

Afin d'assurer l'intégrité de tout le message (non seulement les champs relatifs à la sécurité mais tous les champs de signalisation et de données utilisateur) qui transporte le protocole d'authentification, les expressions cryptées des messages de ces deux versions du protocole peuvent être étendues et contenir, en plus de la valeur du temps, le résultat de la fonction de "hash" des autres champs du message également.

3.2.2. Mode relais

En mode relais le premier message du protocole point à point est le même que celui du protocole d'authentification initiale:

Abonné SA

Appel

jeton_appelant, id_appelant, certificat_appelant, id_service, id_appelé

---------->

jeton_appelant_bis, id_appelant, certificat_appelant

certificat_appelé, ticket_appelant, ticket_appelé

-->

jeton_appelé, certificat_appelé, ticket_appelant

<----------

ou bien

jeton_appelé, certificat_appelé

<----------

jeton_appelé, certificat_appelé, ticket_appelant

<----------

Le deuxième message contient le champ jeton_appelant_bis qui contient la même expression que le champ jeton_appelant dans le cas où la cryptographie à clé publique est utilisée et l'expression suivante si la cryptographie symétrique est utilisée:

$$E(K_{appelé}, K, id\_appelant, temps)$$

Par cette dernière expression le SA assure à l'appelé qu'il a authentifié l'appelant et comme le SA est une (la seule) entité fiable, par transitivité l'appelé a l'assurance de l'identité de l'appelé. Cette expression permet en outre de distribuer la clé secrète partagée K à l'appelé.

Les autres champs des messages ont la même signification que dans le protocole en mode direct et le protocole d'authentification initiale.

Le dernier message de ce protocole peut alternativement transiter par le SA ou être échangé directement entre l'appelé et l'appelant. Ce message n'est d'ailleurs utilisé que si une authentification mutuelle est nécessaire.

4. Correspondance sur le plan fonctionnel distribué (DFP)

Il s'agit de définir l'emplacement des différentes fonctions d'authentification dans le plan fonctionnel distribué du réseau intelligent et de déterminer le flux de messages de signalisation entre les éléments du plan distribué qui transportent les messages d'authentification définis ultérieurement. Il existe ainsi trois schémas de correspondance chacun étant associé à un des trois types de protocoles.

Le rôle du serveur d'authentification est assigné à l'entité Service Control Function (SCF), en distinguant la fonction de contrôle (ou logique du protocole) de la fonction de stockage des données qui est assignée à l'entité Service Data Function (SDF). Les données ainsi stockées sont les clés secrètes des abonnés ($K_{appelant}$, $K_{appelé}$), les clés secrètes des services ($K_{service}$) et les certificats de clés publiques. Dans le cas où le SDF et le SCF doivent communiquer à travers des lignes exposées à l'intrusion et à l'espionnage, il est nécessaire d'établir un canal secret entre ces deux entités.

On distingue aussi la fonction Special Resource Function (SRF) qui réalise des interfaces spécialisées en fonction des caractéristiques des terminaux abonnés.

L'entité Service Management Function (SMF) implémente la fonction d'administration par laquelle la base de données d'authentification est gérée. Les entités Service Switching Function (SSF) prennent en charge la commutation des appels et surtout le déclenchement de la logique du service d'authentification.

La figure 3 présente l'exécution du protocole d'authentification initiale par les entités du DFP.

Figure 3: Protocole d'authentification initiale dans le plan distribué

Dans cette figure les numéros associés aux flèches représentent la séquence des messages échangés dont une description détaillée se trouve ci-dessous:

Message 1: l'abonné déclenche un appel pour un service qui nécessite l'authentification initiale.

Message 2: le commutateur détecte l'appel et contacte le SCF pour le traitement du service.

Message 3: Le SCF (en l'occurrence le SA) demande au SRF d'effectuer un dialogue en utilisant les procédures spécialisées correspondant au terminal de l'abonné. Si une authentification mutuelle est requise ou si l'authentification initiale peut être suivie d'une authentification point à point en mode direct, ce message de signalisation peut transporter le deuxième message du protocole d'authentification initiale. Le fait que le deuxième message est envoyé avant le premier ne pose pas de problème du point de vue de la sécurité.

Messages 4, 5, 6: Le SRF envoie un signal spécialisé (de la voix enregistrée, message de signalisation spécifique à un protocole de carte à puce, etc.) demandant à l'abonné d'envoyer le message correspondant au premier message du protocole d'authentification initiale. Comme dans le cas du message 3, si une

authentification mutuelle est requise ou si l'authentification initiale peut être suivie d'une authentification point à point en mode direct, les messages 4, 5, 6 de signalisation peuvent transporter le deuxième message du protocole d'authentification initiale.

Messages 7, 8, 9, 10: l'abonné envoie le premier message du protocole d'authentification initiale (voir la section sur les protocoles) qui transite par le SSF et le SRF avant d'arriver chez le SCF.

Messages 11, 12: Le SCF obtient les clés et certificats correspondant à l'abonné en questionnant la base de donnée d'authentification. En utilisant ces données et le message envoyé par l'abonné le SCF peut valider l'authentification de l'abonné.

Message 13: Le SCF termine la déviation de l'appel et notifie au SSF de continuer l'acheminement de l'appel (nous supposons que l'authentification a réussi, dans le cas contraire, l'appel serait rejeté à ce niveau).

Messages 14, 15: L'appel est acheminé vers l'abonné appelé ou l'entité de service correspondant au service demandé par l'appel.

La figure 4 représente l'exécution du protocole d'authentification point à point en mode direct. Comme nous l'avons déjà remarqué l'exécution de ce protocole n'implique pas des entités de contrôle du réseau, seules les deux entités aux extrémités de la connexion exécutent le protocole en échangeant le premier message du protocole d'authentification point à point dans le flux des messages de signalisation 1, 2, 3 et le deuxième dans le flux des messages de signalisation 4,5 et 6.

Figure 4: Protocole d'authentification point à point en mode direct

La figure 5 représente l'exécution du protocole d'authentification point à point en mode relais.

Figure 5: Protocole d'authentification point à point en mode relais

Les messages de signalisation numérotés dans cette figure ont la signification suivante:

Message 1: l'abonné déclenche un appel pour un service qui nécessite l'authentification initiale.

Message 2: le commutateur détecte l'appel et contacte le SCF pour le traitement du service.

Message 3: Le SCF (en l'occurrence le SA) demande au SRF d'effectuer un dialogue en utilisant les procédures spécialisées correspondant au terminal de l'abonné.

Messages 4, 5, 6: Le SRF envoie un signal spécialisé (de la voix enregistrée, message de signalisation spécifique à un protocole de carte à puce, etc.) demandant à l'abonné d'envoyer le message correspondant au premier message du protocole d'authentification point à point en mode relais.

Messages 7, 8, 9, 10: l'abonné envoie le premier message du protocole d'authentification en mode relais qui transite par le SSF et le SRF avant d'arriver chez le SCF.

Messages 11, 12: Le SCF obtient les clés et certificats correspondant à l'abonné en questionnant la base de donnée d'authentification. En utilisant ces données et le message envoyé par l'abonné le SCF peut valider l'authentification de l'abonné.

Message 13, 14: Le SCF termine la déviation de l'appel et notifie au SSF de continuer l'acheminement de l'appel (nous supposons que l'authentification a réussi, dans le cas contraire, l'appel serait rejeté à ce niveau). Ce message de signalisation contient aussi le deuxième message du protocole d'authentification en mode relais qui, au lieu d'être transmis directement par le SCF à l'appelé, transitera par la voie d'acheminement de l'appel à travers les commutateurs jusqu'à ce que le dernier commutateur déclenche une procédure d'interface spécialisée en invoquant le SRF.

Messages 15, 16: Le dernier commutateur sur cet appel invoque le SRF en lui transmettant le deuxième message du protocole d'authentification qui avait été généré par le SCF. Le SRF transmet ce message au terminal de l'abonné à travers l'interface spécialisée.

Messages 17, 18: L'abonné appelé ou l'entité interne du service reçoit le deuxième message d'authentification et répond en utilisant le troisième message du protocole. En effet ce dernier message n'est utilisé que si une authentification mutuelle des deux abonnés est effectuée. Dans ce cas le dernier message du protocole peut être acheminé jusqu'à l'abonné appelant par le retour des messages de signalisation ou bien en transitant par le SRF et le SCF.

5. Remarques

La solution présentée dans ce papier a nécessité de faire un choix aussi bien dans la définition des SIB que dans celles des protocoles et de la correspondance sur le plan fonctionnel distribué. Les protocoles à base de nombres aléatoires et des configurations de protocoles autres que celles en mode direct et en mode relais ont été totalement ignorés. Ce choix a été motivé par un souci de simplification. Cependant si ce choix s'avère inadapté pendant les phases ultérieures du projet une ou plusieurs des alternatives qui ont été abandonnées peuvent être reprises.

D'autre part les problèmes abordés n'ont pas été traités entièrement et il reste plusieurs directions suivant lesquelles les solutions doivent être développées plus loin. On peut citer le problème des relations inter-domaines comme un bon exemple des problèmes qui restent à résoudre.

Bibliographie

[1] Authentication method and system with a smartcard, Brevet Européen No. 92810294.6, Refik Molva, Gene Tsudik.