RECOMMANDATION UIT-R M.1223

ÉVALUATION DES MÉCANISMES DE SÉCURITÉ POUR LES IMT-2000

(Question UIT-R 39/8)

(1997)

TABLE DES MATIÈRES

	<i>Page</i>
1 Introduction	2
2 Objet	3
3 Structure de la Recommandation	3
4 Documents connexes	3
5 Définitions	3
6 Considérations	4
7 Recommandations	5
7.1 Exigences concernant les mécanismes de sécurité	5
7.2 Classes de mécanismes de sécurité	5
7.2.1 Mécanismes d'authentification	5
7.2.1.1 Clé symétrique	5
7.2.1.2 Clé asymétrique	6
7.2.1.3 Connaissance zéro	7
7.2.2 Mécanismes garantissant l'anonymat	7
7.2.2.1 Identités temporaires utilisant une clé symétrique	7
7.2.2.2 Confidentialité de l'identité par utilisation d'une clé asymétrique	7
7.2.2.3 Accès anonyme	8
7.2.3 Mécanismes garantissant la confidentialité	8
7.2.3.1 Chiffrement par blocs	8
7.2.3.2 Chiffrement par chaînes	8
7.2.4 Mécanismes de sécurité non cryptographiques	8
7.2.4.1 Vérification de l'identité de l'utilisateur	8
7.2.4.2 Enregistrement	9
7.2.4.3 Comptage des appels	9
7.2.5 Mécanismes garantissant l'intégrité	9
7.2.5.1 Chiffrement	9
7.2.5.2 Clé symétrique	10
7.2.5.3 Clé asymétrique	10
7.2.6 Mécanismes garantissant la non-contestation	10
7.2.7 Gestion de la sécurité	10
7.2.7.1 Gestion des clés	10
7.2.7.2 Gestion des versions	10
Annexe 1 – Mécanismes de sécurité proposés	11
1 Mécanisme d'authentification mutuelle basé sur une fonction de vérification à clé secrète	11
1.1 Fonctions assurées	11
1.2 Exigences de départ	11
1.3 Description du mécanisme	12
1.3.1 Enregistrements existants	12
1.3.2 Enregistrements nouveaux	12

1.4	Évaluation	13
1.4.1	Fourniture de services de sécurité	13
1.4.2	Préfixes – communications	14
1.4.3	Préfixes – administration	14
1.4.4	Préfixes – traitement et autre matériel.....	14
1.4.5	Respect des normes internationales	14
1.4.6	Limitations d'utilisation.....	14
2	Mécanisme d'authentification unilatérale fondé sur l'utilisation de signatures numériques.....	14
2.1	Fonctions assurées	14
2.2	Exigences de départ	14
2.3	Description du mécanisme.....	15
2.3.1	Enregistrements existants.....	15
2.3.2	Nouveaux enregistrements.....	15
2.4	Évaluation.....	16
2.4.1	Fourniture de services de sécurité.....	16
2.4.2	Préfixes – communications	16
2.4.3	Préfixes – administration	16
2.4.4	Préfixes – traitement et autre matériel.....	16
2.4.5	Respect des normes internationales	16
2.4.6	Limitation d'utilisation	16
3	Mécanisme d'authentification unilatérale basé sur l'utilisation de clés publiques.....	16
3.1	Fonctions assurées	17
3.2	Exigences de départ	17
3.3	Description du mécanisme.....	17
3.3.1	Certificat de clé publique	18
3.3.2	Mécanisme d'authentification	18
3.3.3	Variante.....	18
3.4	Évaluation.....	18
3.4.1	Fourniture de services de sécurité.....	18
3.4.2	Préfixes – communications	19
3.4.3	Préfixes – administration	19
3.4.4	Préfixes – traitement et autre matériel.....	19
3.4.5	Respect des normes internationales	19
3.4.6	Limitation d'utilisation	19

1 Introduction

Les télécommunications mobiles internationales-2000 (IMT-2000) sont des systèmes mobiles de la troisième génération dont l'entrée en service est prévue autour de l'an 2000, sous réserve de conditions commerciales. Ils permettront d'accéder, au moyen d'une ou de plusieurs liaisons radioélectriques, à un large éventail de services de télécommunication assurés par des réseaux de télécommunication fixes (par exemple, RTPC/RNIS) ainsi qu'à d'autres services propres aux utilisateurs mobiles.

Ces systèmes utilisent différents types de stations mobiles reliées à des réseaux de Terre et/ou des réseaux à satellites. Ces stations peuvent être conçues pour une utilisation dans le service fixe ou le service mobile.

Les principales caractéristiques des IMT-2000 sont les suivantes:

- grande similitude de conception au niveau mondial;
- compatibilité des services au sein des IMT-2000 et avec les réseaux fixes;

- qualité élevée;
- utilisation d'une petite station de poche pouvant se déplacer au niveau mondial;
- faible coût.

Les IMT-2000 sont définis par un ensemble de Recommandations interdépendantes de l'UIT dont celle-ci fait partie.

Les IMT-2000 sont des systèmes complexes et leur représentation sous forme de Recommandations évolue. Afin de ne pas freiner les progrès accomplis dans ce domaine, il est préférable d'élaborer une série de Recommandations portant sur les divers aspects de ces systèmes tout en s'efforçant d'éviter des contradictions entre elles. Toutefois, si tel était le cas, ces contradictions seraient levées par de nouvelles Recommandations ou par la révision de Recommandations existantes.

Compte tenu de la nature même des radiocommunications hertziennes, il faut doter les IMT-2000 de certains mécanismes de sécurité pour éviter que des personnes non autorisées puissent avoir accès aux données qui sont transmises. De plus, en raison de la nature des communications mobiles, il faut prévoir des mesures de sécurité pour éviter tout accès frauduleux aux services et tout détournement des ressources des fournisseurs ou des exploitants.

2 Objet

La présente Recommandation a pour objet de préciser les différentes catégories de mécanismes de sécurité nécessaires pour mettre en œuvre les fonctions de sécurité des IMT-2000 définies dans la Recommandation UIT-R M.1078 relative aux principes de sécurité pour les IMT-2000 et ainsi satisfaire les exigences de sécurité propres aux IMT-2000 définies dans la même Recommandation. L'Annexe 1 à la présente Recommandation décrit différents mécanismes de sécurité proposés tout en évaluant dans quelle mesure ils peuvent être utilisés dans les IMT-2000.

La présente Recommandation servira de base à l'élaboration de Recommandations plus détaillées sur les mécanismes de sécurité des IMT-2000 dans le cadre des diverses Commissions d'études de l'UIT.

3 Structure de la Recommandation

Le § 7.1 définit un certain nombre de contraintes liées aux mécanismes de sécurité. Le § 7.2 définit diverses catégories de mécanismes de sécurité et examine dans quelle mesure ils peuvent être utilisés pour mettre en œuvre les fonctions de sécurité des IMT-2000 définies dans la Recommandation UIT-R M.1078. L'Annexe 1 décrit plusieurs mécanismes de sécurité proposés pour les IMT-2000 et évalue dans quelle mesure ils sont adaptés à ces systèmes.

4 Documents connexes

Les Recommandations suivantes de l'UIT contiennent des informations sur les IMT-2000 se rapportant à la présente Recommandation:

Recommandation UIT-R M.687:	Télécommunications mobiles internationales-2000 (IMT-2000)
Recommandation UIT-R M.1078:	Principes de sécurité pour les télécommunications mobiles internationales-2000 (IMT-2000)
Recommandation UIT-T F.115:	Objectifs de service et principes relatifs aux futurs systèmes mobiles terrestres publics de télécommunication

5 Définitions

Les sigles suivants sont utilisés dans la présente Recommandation:

IMUI:	identité internationale de l'utilisateur mobile
TMUI:	identité temporaire de l'utilisateur mobile
IMTI:	identité internationale du terminal mobile
TMTI:	identité temporaire du terminal mobile
SPID:	identité du fournisseur de services
NOID:	identité de l'opérateur de réseau

Knu:	clé secrète utilisateur-opérateur de réseau (mécanismes à clé symétriques)
Ksu:	clé secrète utilisateur-fournisseur de services (mécanismes à clé symétriques)
Kpu:	clé de vérification publique de l'utilisateur (mécanismes à clé asymétriques)
Ksignu:	clé à signature privée de l'utilisateur (mécanismes à clé asymétriques)
Kss:	clé à signature privée du fournisseur de services (mécanismes à clé asymétriques)
Kps:	clé de vérification publique du fournisseur de services (mécanismes à clé asymétriques)
Ksn:	clé de déchiffrement privée de l'opérateur de réseau (mécanismes à clé asymétriques)
Kpn:	clé de chiffrement publique de l'opérateur de réseau (mécanismes à clé asymétriques)
Ks:	clé de session
Au:	algorithme d'authentification de l'utilisateur
At:	algorithme d'authentification du terminal
As:	algorithme d'authentification du fournisseur de services
An:	algorithme de production de clé d'opérateur de réseau
Ak:	algorithme de production de clé de session
Cu:	algorithme de dissimulation de l'identité
E:	opération de chiffrement (algorithme de chiffrement à clé publique)
D:	opération de déchiffrement (algorithme de déchiffrement à clé publique)
S:	opération de signature (signature numérique)
V:	opération de vérification (signature numérique)
H:	fonction de brouillage
RND:	essai d'authentification aléatoire
RES:	valeur de contrôle d'authentification
CERT:	certificat
CIFPH:	chaîne de bits servant à dissimuler l'identité
SIG:	signature
KO:	décalage de clé

6 Considérations

Les éléments suivants ont été pris en considération dans l'élaboration de la présente Recommandation:

- a) nécessité d'offrir avec les IMT-2000 une qualité de service comparable à celle offerte par le RTPC/RNIS;
- b) importance de plus en plus grande des divers types de services de télécommunication non téléphoniques;
- c) facilité de réception non seulement pour le destinataire désigné mais pour d'autres personnes en raison de la nature même des communications hertziennes;
- d) compte tenu de la nature même des communications hertziennes, il faut prévoir de mettre en œuvre dans les IMT-2000 des mécanismes garantissant le secret des communications au niveau de l'interface radioélectrique;
- e) compte tenu de la nature des communications mobiles, il faut prendre des mesures concrètes pour éviter tout accès frauduleux aux services et tout détournement des ressources des fournisseurs et des exploitants;
- f) aperçu général du système présenté au § 6 de la Recommandation UIT-R M.1078;
- g) Recommandations UIT-T et UIT-R pertinentes et études en cours;
- h) nécessité de prévoir une structure de système souple garantissant un certain équilibre entre les investissements faits dans le réseau et la croissance des recettes, afin de s'adapter facilement aux paramètres liés à l'environnement et tenir compte de l'évolution sans freiner les innovations;
- j) nécessité pour les terminaux mobiles (y compris ceux dotés de fonctions satellite) de se déplacer entre réseaux de télécommunication mobiles de différents pays;
- k) les IMT-2000 devront fonctionner dans des environnements très divers présentant chacun des caractéristiques de propagation, des densités de trafic et des caractéristiques de mobilité différentes.

7 Recommandations

Les contraintes liées aux mécanismes de sécurité et les différentes catégories de mécanismes de sécurité recommandées pour les IMT-2000 sont indiquées ci-après.

7.1 Exigences concernant les mécanismes de sécurité

- a) Les mécanismes de sécurité devraient nécessiter un minimum de signalisation longue distance en temps réel. Il faudrait, par exemple, éviter de devoir établir des connexions internationales aux fins de signalisation pour chaque appel ou chaque mise à jour de la localisation d'une station en déplacement.
- b) Les mécanismes de sécurité devraient nécessiter un minimum d'arrangements préalables bilatéraux entre fournisseurs de services et opérateurs de réseau.
- c) Les mécanismes de sécurité devraient permettre de gérer les clés cryptographiques que devront éventuellement s'échanger les fournisseurs de services et les opérateurs de réseau.
- d) Les mécanismes de sécurité dont ont besoin les utilisateurs devraient permettre de distribuer et de changer aisément les clés cryptographiques.
- e) Les mécanismes de sécurité devraient être normalisés uniquement dans la mesure nécessaire pour assurer l'interopérabilité et le suivi des déplacements des terminaux.
- f) Les mécanismes de sécurité devraient prévoir une gestion de contrôle des versions afin d'améliorer ou de revoir les mécanismes.
- g) Les mécanismes de sécurité devraient permettre de détecter et de signaler les violations de la sécurité et de rétablir le système dans un état sûr.
- h) Les mécanismes de sécurité devraient respecter les exigences juridiques imposées par les autorités nationales, par exemple contrôle à l'exportation, interception régulière.
- j) Les mécanismes de sécurité devraient permettre de traiter de façon indépendante les fonctions de sécurité liées à l'utilisateur et celles liées au terminal afin que les IMT-2000 puissent assurer à la fois la mobilité de l'utilisateur chaque fois qu'elle est nécessaire, et la mobilité du terminal.

7.2 Classes de mécanismes de sécurité

Les fonctions de sécurité indiquent le type de sécurité qui est assurée alors que les mécanismes de sécurité indiquent comment cette sécurité est assurée. Le présent paragraphe détermine diverses classes de mécanismes de sécurité et examine dans quelle mesure ces mécanismes assurent les fonctions de sécurité que devront remplir les IMT-2000. Les différentes classes identifiées sont calquées, chaque fois que cela est possible, sur la classification utilisée par l'ISO. Les éventuels avantages et inconvénients des différentes méthodes sont indiqués.

Les descriptions des différentes classes de mécanismes présentées ci-après sont des descriptions très générales. Des descriptions plus détaillées de mécanismes particuliers sont données dans l'Annexe 1. Les différents mécanismes sont classés selon la fonction de sécurité qu'ils exécutent le mieux.

Le terme «entité» sera utilisé dans l'ensemble de la Recommandation pour indiquer indifféremment un utilisateur, un terminal, un fournisseur de services, un opérateur de réseau, etc.

7.2.1 Mécanismes d'authentification

Dans les mécanismes de sécurité, il est essentiel de faire la distinction entre les mécanismes dits «symétriques» (ou à clé secrète) et les mécanismes dits «asymétriques» (ou à clé publique). Les mécanismes à clé symétriques ont été utilisés avec succès dans les systèmes mobiles en service. Les mécanismes à clé asymétriques, bien que n'ayant jamais été utilisés dans les systèmes mobiles, ont déjà donné de bons résultats dans les réseaux informatiques existants.

7.2.1.1 Clé symétrique

Dans des mécanismes à clé symétriques, une clé secrète est associée à chaque entité. Les clés ne sont remises qu'à l'entité propriétaire ou à des entités jouissant de la confiance du propriétaire. Elles doivent être mises en mémoire de manière sûre, éventuellement dans un module d'identité d'utilisateur (UIM) – par exemple, une carte à mémoire – ou dans une base de données sûre. L'authentification repose sur le principe que la clé secrète d'une entité n'est connue que de cette entité et d'un nombre limité d'entités en qui l'entité propriétaire a toute confiance, par exemple, celles qui souhaitent authentifier le propriétaire.

Pour obtenir l'authentification, l'entité à authentifier doit prouver à l'entité authenticatrice qu'elle connaît la clé secrète, ce qui peut se faire en générant des paires de questions-réponses, éventuellement en utilisant en entrée la clé secrète (avec d'autres données) d'un algorithme cryptographique unidirectionnel.

Avantages:

- pour une authentification entre un utilisateur et un opérateur de réseau, il est possible d'utiliser des algorithmes propres au fournisseur de services. Si l'opérateur de réseau reçoit du fournisseur de services des paramètres d'authentification préalablement calculés, l'algorithme d'authentification peut être un algorithme propre au fournisseur de services. Sinon, si l'opérateur de réseau reçoit une clé d'authentification (temporaire) l'algorithme de calcul de la clé d'authentification peut être un algorithme propre au fournisseur de service;
- peut être facilement adapté pour calculer des clés de session;
- les algorithmes sont relativement simples et rapides;
- le volume de données nécessaire pour l'authentification est peu important.

Inconvénients:

- il faut disposer de bases de données sûres dans le réseau;
- si l'opérateur de réseau reçoit une clé d'authentification temporaire, il faut alors utiliser un algorithme d'authentification normalisé dans tous les réseaux et les UIM;
- il peut être difficile d'adapter les mécanismes pour assurer l'authentification entre entités arbitraires, car il est nécessaire de distribuer les clés secrètes;
- il doit exister une relation de confiance entre le fournisseur de services et les opérateurs de réseau pour l'échange des clés ou des mécanismes d'authentification préalablement calculés;
- il faut assurer une communication sûre entre le fournisseur de services et les opérateurs de réseau;
- il peut être plus difficile d'assurer d'autres fonctions, par exemple la tarification incontestable et la confidentialité de l'identité de l'utilisateur.

7.2.1.2 Clé asymétrique

Dans les mécanismes à clé asymétriques, chaque entité à authentifier a une clé publique et une clé secrète. Cette clé secrète n'est connue que du propriétaire (utilisateur ou composante du réseau) alors que la clé publique peut être distribuée.

L'entité à authentifier prouve à l'entité effectuant l'authentification qu'elle connaît la clé secrète appropriée. En règle générale, l'authentification se fait comme suit: pour assurer l'authentification, l'entité qui demande l'authentification utilise sa clé secrète pour calculer les informations d'authentification appropriées à partir de données d'entrée d'authentification bien précises. L'entité procédant à la vérification peut alors utiliser la clé publique correspondante aux fins de vérification.

Il existe plusieurs méthodes de distribution de la clé publique. Par exemple, une entité peut posséder un certificat, calculé par une entité en qui elle a toute confiance, qui prouve l'authenticité de la clé publique. Ce certificat peut alors être distribué, si nécessaire. Il peut également y avoir dans le réseau, une base de données regroupant les certificats pour toutes les entités. Dans un cas comme dans l'autre, il faut qu'il existe une autre entité en qui on a toute confiance pour calculer les certificats ou gérer la base de données. Une autre solution consiste à installer préalablement à l'intérieur d'une entité les clés publiques des éventuels partenaires de communication.

Avantages:

- il n'est pas nécessaire de mettre en mémoire ou de transmettre des clés d'authentification secrètes dans un réseau;
- la signalisation au fournisseur de services peut être inutile;
- l'adaptation est facile pour l'authentification entre une paire d'entités;
- la sécurité des communications entre fournisseurs de services et opérateurs de réseau n'est pas nécessaire.

Inconvénients:

- les calculs sont en général plus complexes pour les algorithmes d'authentification;
- les algorithmes proposés sont moins nombreux;
- l'algorithme d'authentification doit être agréé au niveau mondial, même s'il est possible d'utiliser plusieurs versions négociables;
- les échanges de messages ont tendance à être plus longs;
- on aura peut-être besoin d'autorités de certification.

7.2.1.3 Connaissance zéro

Dans cette formule, l'utilisateur a deux identités, une identité publique et une identité secrète correspondante. Ces identités sont créées par le fournisseur de services et enregistrées dans l'UIM. Pour créer les identités, il faut connaître certains paramètres secrets (par exemple, les facteurs d'un grand nombre entier N) mais la relation entre les identités peut être vérifiée à l'aide d'un paramètre qui ne doit pas nécessairement être protégé contre un risque de divulgation (par exemple, l'entier N lui-même).

Pour vérifier l'identité d'une entité, on utilise un protocole de connaissance zéro qui permet à l'entité effectuant la vérification d'avoir la conviction que l'entité connaît l'identité secrète sans que l'entité effectuant la vérification (ou une oreille indiscreète) n'ait connaissance de cette identité même si l'entité effectuant la vérification utilise le protocole à mauvais escient.

Avantage:

- le niveau de sécurité est adaptable.

Inconvénients:

- les mécanismes ont tendance à être complexes;
- il n'est pas facile d'intégrer l'homologation et la distribution des clés de session;
- il faut transmettre des volumes de données importants.

7.2.2 Mécanismes garantissant l'anonymat

7.2.2.1 Identités temporaires utilisant une clé symétrique

Une identité temporaire est disponible et valable uniquement pour une période de temps limitée. Elle peut être exclusive uniquement dans une zone de localisation et peut, par exemple, être réattribuée lors de chaque mise à jour de la localisation.

Une identité temporaire peut être utilisée sur n'importe quelle liaison peu sûre aux fins d'identification, afin de garantir l'anonymat des entités. L'assignation de l'identité temporaire doit être protégée, par exemple par cryptage. Pour certains mécanismes, dans des cas exceptionnels, l'utilisation de l'identité permanente peut être autorisée.

Avantage:

- les identités temporaires sont plus courtes.

Inconvénients:

- l'assignation d'identités temporaires peut nécessiter une gestion supplémentaire afin d'éviter les chevauchements;
- en cas d'erreurs, il faudra éventuellement utiliser l'identité permanente.

7.2.2.2 Confidentialité de l'identité par utilisation d'une clé asymétrique

On peut également garantir la confidentialité de l'identité d'une entité en utilisant un système cryptographique à clé publique.

L'entité peut allonger son identité permanente (par exemple, en lui rajoutant un numéro aléatoire) puis chiffrer ce numéro en utilisant un algorithme à clé publique (par exemple, algorithme RSA (Rivest-Shamir-Adleman)) avec la clé publique du destinataire (opérateur de réseau, fournisseur de services ou utilisateur).

Il faut allonger l'identité pour éviter que des intrus ne recréent l'identité chiffrée et donc vérifient l'identité.

Avantages:

- aucune identité temporaire n'est nécessaire;
- l'identité ne doit jamais être envoyée sans protection.

Inconvénient:

- les identités chiffrées (en utilisant des algorithmes asymétriques) sont plus longues que les identités en clair.

7.2.2.3 Accès anonyme

On pourrait également envisager de recourir à des mécanismes n'utilisant pas l'identification pour assurer l'anonymat, par exemple, l'utilisation d'une carte à prépaiement.

Avantage:

- le risque de divulgation des identités est pratiquement nul.

Inconvénient:

- les scénarios où l'accès anonyme est autorisé sont rares.

7.2.3 Mécanismes garantissant la confidentialité

Un mécanisme de confidentialité peut utiliser un chiffrement par chaînes ou par blocs. La fonction de chiffrement est située en principe dans les terminaux mobiles IMT-2000.

- il faudra éventuellement plus d'un algorithme pour respecter les diverses contraintes juridiques et les contraintes liées à la politique nationale;
- pour le déplacement des stations mobiles, il faudra prévoir une certaine normalisation.

7.2.3.1 Chiffrement par blocs

Le chiffrement par blocs consiste à chiffrer les données d'un champ de longueur fixe à l'aide d'une clé. En principe, les algorithmes de chiffrement par blocs sont utilisés dans le mode opératoire approprié, par exemple, le mode ECB, CBC, CFB ou OFB (voir la Norme ISO/CEI 10116: «Modes opératoires d'un algorithme de chiffrement par blocs de n bits», 1991).

Avantage:

- il existe en principe une documentation importante sur les algorithmes de chiffrement par blocs.

Inconvénients:

- il peut y avoir des erreurs;
- les retards de décryptage sont inévitables.

7.2.3.2 Chiffrement par chaînes

Dans un système de chiffrement par chaînes, une clé est introduite dans un générateur de séquences qui utilise cette clé pour générer une séquence de longueur arbitraire. Cette chaîne de clé est ensuite ajoutée aux données bit par bit.

Avantage:

- il n'y a, en règle générale, pas d'erreurs.

7.2.4 Mécanismes de sécurité non cryptographiques

7.2.4.1 Vérification de l'identité de l'utilisateur

Les mécanismes de vérification permettent de vérifier si l'utilisateur est le véritable utilisateur de l'UIM ou du moins une personne qui jouit de la confiance de l'utilisateur véritable. Si l'UIM est détachable du terminal, ce dernier peut également vérifier l'identité de l'utilisateur. Deux méthodes sont souvent utilisées: un protocole unidirectionnel ou un protocole de question/réponse. En règle générale, les efforts demandés à l'utilisateur sont compensés par le niveau de sécurité réalisé.

L'utilisation d'un numéro d'identité personnel (PIN) est un exemple type de protocole unidirectionnel pour vérifier l'identité d'un utilisateur. Il s'agit d'un numéro secret connu uniquement du propriétaire (ou d'une autre entité autorisée) du terminal de l'UIM et/ou du terminal de l'UIM lui-même. L'utilisateur doit entrer le numéro PIN à l'aide du clavier. Ce numéro PIN est ensuite vérifié dans le terminal/l'UIM.

Un protocole type de question/réponse utilisé pour vérifier l'identité de l'utilisateur est un dialogue au cours duquel le terminal/l'UIM génère un nombre aléatoire de quelques chiffres et l'utilisateur donne le résultat d'un simple calcul avec ce chiffre que le terminal/l'UIM peut vérifier.

Avantage:

- aucune intervention du réseau n'est nécessaire.

Inconvénient:

- une intervention humaine est nécessaire; on ne peut donc utiliser que des mécanismes d'authentification très faibles.

7.2.4.2 Enregistrement

Chaque terminal homologué a une identité de terminal exclusive. Le réseau peut interroger le terminal et lui demander son identité. Sinon, l'identité peut accompagner d'autres données envoyées pendant des procédures particulières. Le réseau met en mémoire des bases de données contenant des listes d'identités de terminal exclusives. La base de données peut comprendre plusieurs listes différentes: une liste blanche, une liste grise et une liste noire. La liste noire contient les identités de terminaux qui ne sont plus autorisés à utiliser le réseau. La liste grise contient les identités de terminaux suspects. La liste blanche contient les identités autorisées.

Chaque réseau peut décider s'il fournit des bases de données de ce type. Des bases de données centrales, contenant tous les terminaux disponibles (au niveau international) et le statut qui leur est associé, sont nécessaires pour permettre l'interfonctionnement et le suivi des déplacements au niveau international.

Avantage:

- peut être utilisé pour détecter un certain nombre de problèmes liés à l'équipement, par exemple, vol, dysfonctionnement, non-homologation.

Inconvénients:

- une identité peut être modifiée et prévisible et elle ne constitue pas une protection contre des clones de terminaux;
- des mises à jour régulières (également au niveau international) sont nécessaires pour avoir des informations fiables;
- des messages de signalisation supplémentaires sont nécessaires.

7.2.4.3 Comptage des appels

Une forme de détection des clones est un paramètre de «comptage des appels» qui peut être mis à jour dans l'UIM, sur commande du réseau. Un compteur similaire sera également mis à jour par le fournisseur de services. S'il apparaît qu'un UIM particulier présente des valeurs de «comptage» discontinues, il est probable qu'un clone soit en train d'usurper l'UIM de l'utilisateur légitime et ait accédé au service avant l'utilisateur légitime. Ce mécanisme ne détecte que les clones d'UIM.

Un «compteur d'appels» pourrait également être lié au terminal et mis à jour dans le terminal et dans une base de données mondiale contenant les identités de terminal et les compteurs d'appels associés. Dans cette variante, il est possible de détecter les clones de terminaux.

Avantage:

- aucun mécanisme de protection physique coûteux n'est nécessaire.

Inconvénients:

- une gestion du comptage des appels peut être nécessaire dans le réseau;
- des messages de signalisation supplémentaires peuvent être nécessaires.

7.2.5 Mécanismes garantissant l'intégrité

7.2.5.1 Chiffrement

Si les données transférées contiennent une redondance suffisante, le chiffrement peut donner l'assurance que les données transmises n'ont pas été modifiées.

Avantage:

- aucune autre dépense que celle liée à la confidentialité.

Inconvénients:

- aucune prévention contre des attaques basées sur le rejeu (il faut ajouter des numéros ou des compteurs aléatoires);
- ne peut être utilisé qu'avec des données très redondantes.

7.2.5.2 Clé symétrique

Il existe deux techniques fondamentales pour assurer l'intégrité d'un message: l'utilisation de codes d'authentification de message (MAC) comprenant une chaîne de données qui est une fonction cryptographique du message et une clé secrète et l'utilisation de codes de détection des manipulations (MDC) comprenant une chaîne de données qui n'est qu'une fonction du message. Étant donné que la fonction de génération du MDC est connue publiquement, il faut crypter au moins le MDC.

Avantage:

- algorithmes relativement simples.

Inconvénients:

- aucune protection contre les attaques basées sur le rejeu (il faut ajouter un numéro ou des compteurs aléatoires);
- il faut connaître les clés secrètes des personnes participant à la communication;
- il existe une protection uniquement contre les attaques de tiers.

7.2.5.3 Clé asymétrique

Une valeur de brouillage du message d'origine est signée avec la clé secrète de l'expéditeur. Cette signature, jointe au message transmis, peut être vérifiée par tout destinataire possédant la clé publique de l'expéditeur.

Avantage:

- n'importe quel tiers peut vérifier les données.

Inconvénients:

- les calculs ont tendance à être plus complexes pour ces algorithmes;
- les algorithmes proposés sont peu nombreux.

7.2.6 Mécanismes garantissant la non-contestation

Des signatures numériques, calculées en fonction de données connues, peuvent être utilisées pour éviter que les données envoyées ou reçues soient contestées.

Les niveaux de non-contestation sont différents selon le volume des données à signer et la façon dont les signatures calculées et les données d'origine sont sauveées et mises en mémoire.

Avantage:

- on peut obtenir différents niveaux de non-contestation.

Inconvénient:

- il faut utiliser des algorithmes asymétriques pour éviter que l'entité procédant à la vérification ne produise de fausses signatures.

7.2.7 Gestion de la sécurité

7.2.7.1 Gestion des clés

Il existe diverses formes de génération, de distribution et de certification des clés. Les exigences à respecter pour la gestion des clés dépendront des mécanismes IMT-2000 particuliers qui ont été choisis pour assurer les fonctions de sécurité IMT-2000.

7.2.7.2 Gestion des versions

La gestion des versions est un mécanisme qui permet au système de mettre à jour ou de remplacer les procédures ou les mécanismes de sécurité sans qu'il soit nécessaire de remplacer les terminaux mobiles IMT-2000 existants. L'utilisation d'UIM amovibles peut s'expliquer, entre autres, par le fait qu'on peut ainsi mettre à jour des mécanismes et des algorithmes en créant de nouveaux UIM (sans toucher aux terminaux).

ANNEXE 1

Mécanismes de sécurité proposés

La présente Annexe décrit en détail plusieurs exemples de mécanismes de sécurité sans les structurer dans l'architecture fonctionnelle des IMT-2000 (voir la Recommandation UIT-R M.817). Ces mécanismes sont indiqués à titre d'illustration et d'autres mécanismes peuvent être appliqués.

1 Mécanisme d'authentification mutuelle basé sur une fonction de vérification à clé secrète

Le présent paragraphe décrit un exemple de mécanisme d'authentification mutuelle reposant sur l'utilisation d'un système cryptographique à clé secrète et sur un échange de questions-réponses et assurant trois fonctions: la confidentialité de l'identité de l'utilisateur, l'authentification de l'entité et la production de clés de session.

1.1 Fonctions assurées

Le mécanisme assure les fonctions de sécurité suivantes:

- Authentification d'entité mutuelle entre l'utilisateur et l'opérateur de réseau.
- Confidentialité de l'identité de l'utilisateur sur le trajet de communication entre l'utilisateur et l'opérateur de réseau.
- Établissement de clés de session entre l'utilisateur et l'opérateur de réseau (utilisées pour fournir d'autres fonctions de sécurité, éventuellement la confidentialité et/ou l'intégrité des données transmises entre l'utilisateur et l'opérateur de réseau).

1.2 Exigences de départ

Le mécanisme utilise les algorithmes cryptographiques suivants:

- L'algorithme d'authentification de l'utilisateur, Au. Cet algorithme prend en compte une clé secrète et une chaîne de données pour produire une valeur de contrôle d'authentification RES.
- L'algorithme d'authentification du fournisseur de services, As. Cet algorithme prend en compte une clé secrète et une chaîne de données pour produire une RES. Il peut s'agir du même algorithme que l'Au ou d'un algorithme différent.
- L'algorithme de dissimulation de l'identité, Cu. Cet algorithme prend en compte une clé secrète et une chaîne de données pour produire une chaîne de bits servant à dissimuler l'identité, CIPH de l'utilisateur.
- L'algorithme de production de clé de session, Ak. Cet algorithme prend en compte une clé secrète et une chaîne de données pour produire une clé de session Ks.
- L'algorithme de production de clé d'opérateur de réseau, An. Cet algorithme prend en compte une clé secrète et une chaîne de données pour produire une clé secrète utilisateur-opérateur de réseau, Knu. Il peut s'agir du même algorithme que l'algorithme Ak ou d'un algorithme différent.

Le mécanisme utilise les types de clé cryptographique suivants:

- Clé secrète utilisateur-fournisseur de services, Ksu. Il s'agit de clés secrètes connues uniquement de l'utilisateur et du fournisseur de services qui lui est associé. Ces clés secrètes restent inchangées pendant de longues périodes de temps.
- Clé secrète utilisateur-opérateur de réseau, Knu. Il s'agit de clés secrètes connues uniquement de l'utilisateur et de l'opérateur de réseau «concerné» qui lui est associé. Ces clés peuvent rester inchangées alors que l'utilisateur est enregistré auprès d'un opérateur de réseau particulier. Associé à chaque clé de ce type, il y a un décalage de clé, KO, utilisé avec la clé secrète utilisateur-fournisseur de services, Ksu pour produire une clé Knu.
- Clé de session, Ks. Il s'agit de clés secrètes connues uniquement de l'utilisateur et de l'opérateur de réseau concerné (c'est-à-dire l'opérateur de réseau auquel l'utilisateur est rattaché). Une nouvelle Ks est produite après chaque utilisation du mécanisme d'authentification. Ces clés peuvent être utilisées pour le chiffrement des données et/ou la fourniture d'autres fonctions de sécurité.

Le mécanisme utilise les types d'identificateur suivants:

- Identité internationale de l'utilisateur mobile, IMUI. Il s'agit d'une identité associée de façon permanente à un utilisateur. L'identité IMUI ne traverse jamais l'interface radioélectrique ce qui évite qu'elle ne soit divulguée sans autorisation.
- Identité de l'opérateur de réseau, NOID.
- Identité de l'utilisateur temporaire pour l'opérateur de réseau TMUIn. Cette identité (temporaire) sert à identifier un utilisateur auprès de l'opérateur de réseau auquel il est rattaché. Elle est connue de l'utilisateur et de l'opérateur du réseau IMT-2000 concerné.
- Identité de l'utilisateur temporaire pour le fournisseur de service TMUIs. Cette identité (temporaire) sert à identifier un utilisateur auprès de son fournisseur de service. Elle est connue de l'utilisateur et de son fournisseur de service.

La contrainte suivante est associée au mécanisme:

- L'opérateur de réseau et le fournisseur de services ont besoin d'un canal sûr pour échanger le deuxième et le troisième messages de la version «nouvel enregistrement» du mécanisme.

1.3 Description du mécanisme

Il existe deux versions du mécanisme selon que l'utilisateur est enregistré ou non auprès de l'opérateur de réseau. Les deux cas sont envisagés séparément (même s'ils sont étroitement liés).

1.3.1 Enregistrements existants

Considérons tout d'abord le cas où l'utilisateur est déjà enregistré auprès de l'opérateur de réseau, ce qui signifie que l'utilisateur et l'opérateur de réseau partageront une identité temporaire valable TMUIn et une clé secrète Knu. Dans ce cas, le mécanisme consiste en l'échange de trois messages entre l'utilisateur et l'opérateur de réseau. Le fournisseur de service n'est pas concerné.

Les trois messages sont les suivants:

Message 1: utilisateur → opérateur de réseau: TMUIn, RNDu

Message 2: opérateur de réseau → utilisateur: RNDn, KO, TMUIn'+CIPHn, RESn

Message 3: utilisateur → opérateur de réseau: RESu.

On notera que le signe + apparaissant dans les messages ci-dessus signifie l'adjonction binaire bit par bit de deux chaînes.

Les valeurs RNDu et RNDn sont des «questions» aléatoires générées respectivement par l'utilisateur et l'opérateur de réseau.

Les valeurs RESu et RESn sont des «réponses aux questions» générées respectivement par l'utilisateur et l'opérateur de réseau. On calcule la valeur RESn en utilisant l'algorithme Au qui prend en compte comme clé la clé Knu et comme chaîne de données la concaténation de RNDn et RNDu et TMUIn'. On calcule la valeur RESu en utilisant l'algorithme Au, qui prend en compte comme clé la clé Knu et comme chaîne de données la concaténation de RNDu et RNDn.

L'identité TMUIn' est la «nouvelle» identité temporaire de l'utilisateur à utiliser auprès de l'opérateur de réseau. Elle remplacera l'identité temporaire existante TMUIn.

La chaîne CIPHn est une chaîne de bits servant à dissimuler la nouvelle identité temporaire TMUIn' pendant qu'elle transite entre l'opérateur de réseau et l'utilisateur. On la calcule en utilisant l'algorithme de dissimulation de l'identité, Cu, qui prend en compte comme clé la clé secrète Knu et comme chaîne de données le paramètre RNDu.

L'utilisateur et l'opérateur de réseau peuvent calculer une clé de session Ks en utilisant l'algorithme Ak, qui prend en compte comme clé la clé secrète Knu et comme chaîne de données la concaténation de RNDu, RNDn et RMUIn'.

Les paramètres RNDu et RESn ne seront pas utilisés dans le cas particulier d'une authentification unidirectionnelle et d'une dissimulation d'identité. Dans ce cas, on calcule le paramètre CIPHn en utilisant l'algorithme Cu qui prend en compte comme clé la clé secrète Knu et comme chaîne de données le paramètre RNDn.

1.3.2 Enregistrements nouveaux

Considérons maintenant le cas où l'utilisateur n'est pas enregistré auprès de l'opérateur de réseau, ce qui signifie que l'utilisateur et l'opérateur de réseau ne partagent aucune information. Dans ce cas, le mécanisme consiste en l'échange de cinq messages entre l'utilisateur, l'opérateur de réseau et le fournisseur de service de l'utilisateur.

Les cinq messages sont les suivants:

Message 1: utilisateur → opérateur de réseau: TMUIs, RNDu
Message 2: opérateur de réseau → fournisseur de service: TMUIs, RNDu
Message 3: fournisseur de service → opérateur de réseau: TMUIs'+CIPHs, KO, Knu, RESs
Message 4: opérateur de réseau → utilisateur: TMUIs'+CIPHs, RESs, RNDn, KO, TMUIn'+CIPHn, RESn
Message 5: utilisateur → opérateur de réseau: RESu

On notera tout d'abord que, par hypothèse, on suppose qu'il existe un canal sûr pour échanger les messages 2 et 3 entre l'opérateur de réseau et le fournisseur de service.

Comme dans le cas précédent, les valeurs RNDu et RNDn sont des «questions» aléatoires générées respectivement par l'utilisateur et l'opérateur de réseau.

Les valeurs RESu, RESn et RESs sont des «réponses aux questions» générées respectivement par l'utilisateur, l'opérateur de réseau et le fournisseur de service. On calcule les paramètres RESn et RESu comme dans le cas précédent. On calcule le paramètre RESs en utilisant l'algorithme As qui prend en compte comme clé la clé Ksu et comme chaîne de données la concaténation de RNDu et TMUIs'.

L'identité TMUIs' est la «nouvelle» identité temporaire de l'utilisateur à utiliser auprès du fournisseur de services. Elle remplacera l'identité temporaire existante TMUIs. Comme précédemment l'identité TMUIn' est la «nouvelle» identité temporaire de l'utilisateur à utiliser auprès de l'opérateur de réseau.

La chaîne CIPHs est une chaîne de bits servant à dissimuler la nouvelle identité temporaire TMUIs' lorsqu'elle transite entre le fournisseur de services et l'utilisateur. On la calcule en utilisant l'algorithme de dissimulation de l'identité, Cu, qui prend en compte comme clé la clé secrète Ksu et comme chaîne de données le paramètre RNDu. Comme précédemment, la chaîne CIPHn sert à dissimuler la nouvelle identité temporaire TMUIn' alors qu'elle transite entre l'opérateur de réseau et l'utilisateur.

Lorsqu'il reçoit le message 4, l'utilisateur peut calculer la clé secrète Knu de l'opérateur de réseau en utilisant l'algorithme An, qui prend en compte comme clé la clé secrète Ksu et comme chaîne de données le décalage de clé KO concaténé à l'identité de l'opérateur de réseau NOID (le fournisseur de services effectue le même calcul lorsqu'il reçoit le message 2).

Comme précédemment, l'utilisateur et l'opérateur de réseau peuvent calculer une clé de session Ks en utilisant l'algorithme Ak, qui prend en compte comme clé la clé secrète Knu et comme chaîne de données la concaténation de RNDu, RNDn et TMUIn'.

Résultat de l'application de ce mécanisme, l'utilisateur et l'opérateur de réseau partageront une clé secrète Knu et une identité temporaire TMUIn'. On notera également que dans le mécanisme décrit ci-dessus, l'identité IMUI de l'utilisateur n'est pas communiquée automatiquement à l'opérateur de réseau. Si cela est nécessaire pour des raisons juridiques et/ou d'exploitation, cette identité peut être incluse dans le troisième message du mécanisme d'authentification «nouvel enregistrement».

Les paramètres RNDu et RESn ne seront pas utilisés dans le cas particulier d'authentification unidirectionnelle utilisateur-réseau et de dissimulation d'identité. Dans ce cas particulier toutefois, les messages 3 et 4 doivent acheminer en plus des paramètres indiqués ci-dessus le paramètre RNDs, «question» aléatoire générée par le fournisseur de services. Par ailleurs, on calcule la chaîne CIPHs en utilisant l'algorithme Cu qui prend en compte comme clé la clé secrète Ksu et comme chaîne de données le paramètre RNDs; on calcule la chaîne CIPHn en utilisant l'algorithme Cu qui prend en compte comme clé la clé secrète Knu et comme chaîne de données le paramètre RNDn.

1.4 Évaluation

Le mécanisme a les caractéristiques significatives suivantes.

1.4.1 Fourniture de services de sécurité

Il apparaît que le mécanisme de sécurité fournit les services pour lesquels il a été conçu. Des preuves de sécurité en bonne et due forme ont été créées pour le mécanisme. Il est relativement simple de créer des fonctions de contrôle appropriées.

1.4.2 Préfixes – communications

Il faut pour les deux versions du mécanisme respectivement trois et cinq messages. C'est le nombre minimal nécessaire pour l'authentification mutuelle étant donné que le fournisseur de services doit être consulté et que l'on n'utilise pas de marques d'horodatage (les deux autres services sont fournis sans qu'il soit nécessaire d'envoyer de messages supplémentaires). Tous les messages seront relativement courts.

1.4.3 Préfixes – administration

Dans ce mécanisme, les entités sont tenues de mettre en mémoire des questions aléatoires pendant de brèves périodes de temps. Les identités temporaires et les clés devront elles aussi être mises en mémoire. Le fournisseur de services n'est pas nécessairement concerné; son intervention est limitée au cas où un utilisateur souhaite utiliser un nouvel opérateur de réseau.

1.4.4 Préfixes – traitement et autre matériel

Il est possible de faire en sorte que tous les algorithmes cryptographiques soient simples à calculer.

1.4.5 Respect des normes internationales

La version à trois passages du mécanisme est conforme à la norme ISO/CEI 9798-4: 1995 (à condition que les éléments des messages soient assemblés dans le bon ordre).

1.4.6 Limitations d'utilisation

Le mécanisme n'utilise que des fonctions de vérification et n'utilise pas des opérations de chiffrement. La mobilité transfrontière de l'équipement mettant en œuvre ce mécanisme sera donc, vraisemblablement simplifiée. Il n'y a aucune restriction en matière de brevets.

2 Mécanisme d'authentification unilatérale fondé sur l'utilisation de signatures numériques

Le présent paragraphe décrit un exemple de mécanisme d'authentification unilatérale reposant sur l'utilisation d'une signature numérique et d'un échange de questions-réponses et assurant deux fonctions: la confidentialité de l'identité de l'utilisateur et l'authentification unilatérale de l'entité.

2.1 Fonctions assurées

Le mécanisme assure les fonctions de sécurité suivantes:

- Authentification d'entité unilatérale de l'utilisateur auprès de l'opérateur de réseau.
- Confidentialité de l'identité de l'utilisateur sur le trajet de communication entre l'utilisateur et l'opérateur de réseau.

2.2 Exigences de départ

Le mécanisme utilise les algorithmes cryptographiques suivants:

- Algorithme à signature numérique de l'utilisateur. Cet algorithme comprend deux opérations, la signature S et la vérification V . L'opération de signature prend en compte une clé à signature privée et une chaîne de données pour produire une signature SIG . L'opération de vérification prend en compte une clé de vérification publique, une signature SIG et une chaîne de données pour produire une valeur binaire (oui/non) indiquant si la signature SIG d'entrée est une signature valable pour la chaîne de données d'entrée.

Le mécanisme utilise les types de clés cryptographiques suivants:

- Clé à signature privée de l'utilisateur, K_{sigu} . Il s'agit de clés privées connues uniquement de l'utilisateur. Elles restent inchangées pendant de longues périodes de temps. Elles sont prises en compte pour l'opération de signature, S , de l'utilisateur.
- Clé de vérification publique de l'utilisateur, K_{pui} . Il s'agit de clés publiques qui peuvent être connues de nombreux opérateurs de réseau. Elles seront prises en compte pour l'opération de vérification, V , publique.

Le mécanisme utilise les types d'identificateurs suivants:

- Identité internationale de l'utilisateur mobile, IMUI. Il s'agit d'une identité associée de façon permanente à l'utilisateur. L'identité IMU n'est jamais acheminée à travers l'interface radioélectrique, ce qui évite qu'elle ne soit divulguée sans autorisation.
- Identité temporaire de l'utilisateur mobile, TMUI. Cette identité (temporaire) sert à identifier un utilisateur auprès de l'opérateur de réseau auprès duquel il est enregistré. Elle est connue de l'utilisateur et de l'opérateur de réseau IMT-2000 concerné.

2.3 Description du mécanisme

Il existe deux versions du mécanisme selon que l'utilisateur est enregistré ou non auprès de l'opérateur de réseau. Nous examinerons les deux cas séparément.

2.3.1 Enregistrements existants

Considérons tout d'abord le cas où l'utilisateur est déjà enregistré auprès de l'opérateur de réseau, ce qui signifie que l'utilisateur et l'opérateur de réseau partageront une identité temporaire valable TMUI et que l'opérateur de réseau aura une copie de la clé de vérification publique de l'utilisateur, Kpu. Dans ce cas, le mécanisme consiste en l'échange de trois messages entre l'utilisateur et l'opérateur de réseau. Le fournisseur de services n'est pas concerné.

Les trois messages sont les suivants:

Message 1: utilisateur → opérateur de réseau: TMUI

Message 2: opérateur de réseau → utilisateur: RNDn

Message 3: utilisateur → opérateur de réseau: RNDn, RESu.

La valeur RNDn est une «question» aléatoire générée par l'opérateur de réseau.

La valeur RNDu est un nombre aléatoire généré par l'utilisateur.

La valeur RESu est une «réponse à la question» générée par l'utilisateur. On calcule cette valeur en utilisant l'opération de signature S qui prend en compte la clé Ksigu et la chaîne de donnée formée par la concaténation de RNDn et RNDu.

Lorsqu'il reçoit l'identité TMUI, l'opérateur de réseau génère de façon aléatoire la valeur RNDn et la met en mémoire, en vue d'une vérification ultérieure. Cette valeur est envoyée à l'utilisateur comme deuxième message du mécanisme.

Lorsqu'il reçoit la valeur RNDn, l'utilisateur génère de façon aléatoire la valeur RNDu. Les valeurs RNDn et RNDu sont utilisées pour générer la valeur RESu qui est envoyée à l'opérateur de réseau dans le troisième message du mécanisme.

Lorsqu'il reçoit la valeur RESu, l'opérateur de réseau l'utilise comme signature SIG d'entrée pour l'opération de vérification V qui prend en compte comme chaîne de données la concaténation de la valeur RESn mise en mémoire, et de la valeur RESu reçue et comme clé la clé Kpu. Le résultat de l'opération V servira à déterminer si l'identité de l'utilisateur est correcte.

2.3.2 Nouveaux enregistrements

Considérons maintenant le cas où l'utilisateur n'est pas enregistré auprès de l'opérateur de réseau, ce qui signifie que l'utilisateur et l'opérateur de réseau ne partagent aucune information. Dans ce cas, le mécanisme reste à spécifier. Les exigences liées à ce mécanisme sont les suivantes.

- L'utilisateur et l'opérateur de réseau doivent avoir une identité TMUI pour que l'utilisateur puisse s'identifier auprès de l'opérateur de réseau, au niveau de l'interface radioélectrique sans affecter la valeur de son identité IMUI.
- L'opérateur de réseau doit avoir une copie de clé Kpu.

En théorie, ces exigences devraient être respectées sans qu'il soit nécessaire de transmettre l'identité IMUI de l'utilisateur et/ou un certificat de clé publique pour l'utilisateur au niveau de l'interface radioélectrique (à moins que ces valeurs ne soient chiffrées d'une façon ou d'une autre).

2.4 Évaluation

Le mécanisme a les caractéristiques significatives suivantes.

2.4.1 Fourniture de services de sécurité

Il apparaît que le mécanisme de sécurité assure le service d'authentification pour lequel il a été conçu. Toutefois, la fourniture de la confidentialité de l'identité de l'utilisateur est plus incertaine. En effet, le mécanisme ne prévoit pas de mise à jour d'une identité TMUI; si la même identité TMUI est utilisée de façon répétée, il se peut qu'un intercepteur lie tous les éléments de trafic correspondant à un seul particulier, ce qui pourrait compromettre en partie le bon fonctionnement du service de confidentialité de l'identité.

L'«initialisation» du mécanisme pose également un problème. Il faut mettre au point une méthode pour le traitement des nouveaux enregistrements. Le problème n'est toutefois pas insurmontable et on pourrait mettre au point un mécanisme pour les nouveaux enregistrements en utilisant une variante du mécanisme décrit dans le paragraphe suivant.

Il existe un certain nombre d'algorithmes à signature numérique adaptés. Le fait d'utiliser le deuxième nombre aléatoire, Ru, dans le calcul de la valeur RESu signifie que l'utilisateur évite de fournir à l'opérateur de réseau la version signée d'une chaîne de données spécifiée dans son intégralité par l'opérateur de réseau. Si la même clé de signature est utilisée pour signer d'autres types de données, la sécurité ne serait plus assurée. Si tel n'est pas le cas, le nombre aléatoire RNDu pourrait être ramené à zéro, c'est-à-dire avoir une longueur égale à zéro.

2.4.2 Préfixes – communications

Dans ce mécanisme, trois messages doivent être envoyés. En fait, il est possible de mettre au point avec ce nombre de messages, un mécanisme d'authentification mutuelle reposant sur un jeu de questions-réponses; par ailleurs, s'il est «initialisé» par l'opérateur de réseau, un mécanisme d'authentification unilatérale ne nécessitant que deux messages peut facilement être mis au point. Le service de confidentialité de l'identité est assuré sans qu'il soit nécessaire d'envoyer d'autres messages. Tous les messages seront relativement brefs, à l'exception du troisième message; dans ce message, le champ SIG contient en général entre 512 et 1 024 bits.

2.4.3 Préfixes – administration

Dans ce mécanisme, les entités sont tenues de mettre en mémoire des questions aléatoires pendant de brèves périodes de temps. Les identités temporaires et les clés devront elles aussi être mises en mémoire. Le fournisseur de services n'est pas nécessairement concerné; son intervention est limitée au cas où un utilisateur souhaite utiliser un nouvel opérateur de réseau.

La taille des clés pour l'algorithme à signature numérique est en général assez importante (1 024 bits ou plus) comparée à celle des clés pour des algorithmes classiques (64-128 bits).

2.4.4 Préfixes – traitement et autre matériel

Les calculs pour les opérations de signature et de vérification peuvent être assez complexes; cette complexité dépendra de l'algorithme et de la taille des clés utilisées.

2.4.5 Respect des normes internationales

Le mécanisme est conforme à la Norme ISO/CEI 9798-3: 1993 (à condition que les éléments des messages soient assemblés dans le bon ordre).

2.4.6 Limitation d'utilisation

Le mécanisme utilise uniquement une fonction de signature numérique et n'utilise pas d'opérations de chiffrement. La mobilité transfrontière de l'équipement mettant en œuvre ce mécanisme sera donc, vraisemblablement, facilitée. Le mécanisme lui-même ne fait l'objet d'aucune restriction en matière de brevets, même si certains algorithmes à signature numérique sont couverts par des brevets.

3 Mécanisme d'authentification unilatérale basé sur l'utilisation de clés publiques

Le présent paragraphe décrit un exemple de mécanisme d'authentification unilatérale reposant sur l'utilisation d'une signature numérique, d'une méthode de chiffrement à clé publique, de certificats de clé publique et de marques d'horodatage et assurant deux fonctions: la confidentialité de l'identité de l'utilisateur et l'authentification d'entité unilatérale.

3.1 Fonctions assurées

Le mécanisme assure les fonctions de sécurité suivantes:

- Authentification d'entité unilatérale de l'utilisateur auprès de l'opérateur de réseau.
- Confidentialité de l'identité de l'utilisateur sur le trajet de communication entre l'utilisateur et l'opérateur de réseau.

3.2 Exigences de départ

Le mécanisme utilise les algorithmes cryptographiques suivants:

- Algorithme à signature numérique. Cet algorithme comprend deux opérations, la signature S et la vérification V. L'opération de signature prend en compte une clé à signature privée et une chaîne de données pour produire une signature, SIG. L'opération de vérification prend en compte une clé de vérification publique, une signature SIG et une chaîne de données pour produire une valeur binaire (oui/non) indiquant si la signature SIG d'entrée est une signature valable pour la chaîne de données d'entrée.
- Algorithme de chiffrement à clé publique. Cet algorithme comprend deux opérations, le chiffrement E et le déchiffrement D. L'opération de chiffrement prend en compte une clé de chiffrement publique et une chaîne de données pour produire une chaîne de données chiffrée. L'opération de déchiffrement prend en compte une clé de déchiffrement privée et une chaîne de données chiffrée et sort une chaîne de données non codée.

Le mécanisme utilise les types de clés cryptographiques suivants:

- Clé à signature privée de l'utilisateur, Ksigu. Il s'agit d'une clé privée connue uniquement de l'utilisateur. Ces clés privées restent inchangées pendant de longues périodes de temps. Elles sont prises en compte pour l'opération de signature S.
- Clé de vérification publique de l'utilisateur, Kpu. Il s'agit d'une clé publique connue du fournisseur de services de l'utilisateur. Ces clés sont prises en compte pour l'opération de vérification V.
- Clé à signature privée du fournisseur de services, Kss. Il s'agit d'une clé privée connue uniquement du fournisseur de services. Ces clés restent inchangées pendant de longues périodes de temps. Elles sont prises en compte pour l'opération de signature S.
- Clé de vérification publique du fournisseur de services, Kps. Il s'agit d'une clé publique connue de tous les opérateurs de réseau ayant conclu un accord de fourniture de services avec un fournisseur de services. Ces clés sont prises en compte pour l'opération de vérification V.
- Clé de déchiffrement privée de l'opérateur de réseau, Ksn. Il s'agit de clés privées connues uniquement de l'opérateur de réseau. Elles restent inchangées pendant de longues périodes de temps. Elles sont prises en compte pour l'opération de déchiffrement à clé publique D.
- Clé de chiffrement publique de l'opérateur de réseau, Kpn. Il s'agit de clés publiques connues de tous les utilisateurs qui souhaitent utiliser un opérateur de réseau. Elles sont prises en compte pour l'opération de chiffrement à clé publique E.

Le mécanisme utilise les types d'identificateurs suivants:

- Identité internationale de l'utilisateur mobile, IMUI. Il s'agit d'une identité associée de façon permanente à un utilisateur. L'identité IMUI n'est jamais transmise à travers l'interface radioélectrique, ce qui évite qu'elle soit divulguée sans autorisation.
- Identité temporaire de l'utilisateur mobile, TMUI. Cette identité (temporaire) sert à identifier un utilisateur auprès de l'opérateur de réseau auprès duquel il est enregistré. Elle est connue de l'utilisateur et de l'opérateur de réseau IMT-2000 concerné.
- Identité du fournisseur de services, SPID.

Une contrainte supplémentaire est associée au mécanisme:

- Les utilisateurs, les opérateurs de réseau et les fournisseurs de services doivent tous avoir des horloges synchronisées.

3.3 Description du mécanisme

Il existe une seule version du mécanisme décrit ci-après.

À la différence du cas précédent, ce mécanisme n'exige pas que l'utilisateur soit déjà enregistré auprès de l'opérateur de réseau. Dans ce cas, le mécanisme se compose d'un message que l'utilisateur envoie à l'opérateur de réseau. Le fournisseur de services n'est pas concerné. Toutefois, il faut que ce dernier envoie un certificat de clé publique à l'utilisateur. Examinons tout d'abord la forme du certificat avant de décrire le mécanisme lui-même.

3.3.1 Certificat de clé publique

Le certificat pour un utilisateur, CERTu, est la concaténation des chaînes de données suivantes:

- l'identité IMUI;
- l'identité SPID;
- la date de délivrance du certificat;
- la durée de validité du certificat;
- la clé Kpu;
- le produit de l'opération de signature S qui prend en compte la clé à signature privée du fournisseur de services et la chaîne de données formée par la concaténation des identités IMUI et SPID, de la date de délivrance, de la durée de validité du certificat et de la clé Kpu.

L'utilisateur peut alors fournir le certificat à n'importe quel opérateur de réseau qui peut s'en servir pour obtenir une copie certifiée conforme de la clé publique de l'utilisateur, sans intervention du fournisseur de services de l'utilisateur.

3.3.2 Mécanisme d'authentification

Le message que l'utilisateur envoie à l'opérateur de réseau est le suivant:

- utilisateur → opérateur de réseau: AUTH

La valeur AUTH est le produit de l'opération de chiffrement de clé publique E qui prend en compte comme clé la clé Kpn, et comme chaîne de données celle formée par la concaténation du certificat de l'utilisateur CERTu, de la marque d'horodatage Tu et de la valeur RESu.

La valeur RESu est calculée comme étant le produit de l'opération de signature S qui prend en compte comme clé la clé Ksigu, et comme chaîne de données la marque l'horodatage Tu.

La marque d'horodatage Tu est générée à partir de l'horloge de l'utilisateur.

Lorsqu'il reçoit le message AUTH de l'utilisateur, l'opérateur de réseau tout d'abord le déchiffre en utilisant l'opération de déchiffrement à clé publique avec la clé Ksn. Il obtient CERTu, Tu et RESu. L'opérateur de réseau effectue alors les opérations suivantes.

- La marque d'horodatage Tu est vérifiée pour voir si elle est actuelle, c'est-à-dire si elle se situe dans les limites de la «fenêtre d'acceptation».
- L'opérateur de réseau utilise maintenant la clé Kps pour vérifier la signature à l'intérieur du certificat. Si les contrôles sont bons, la période de validité du certificat est également vérifiée.
- Enfin, la valeur RSU est introduite en entrée dans l'opération de vérification (comme signature d'entrée) qui prend en compte comme chaîne de données d'entrée la marque d'horodatage Tu et comme clé la clé Kpu.
- Si tous les contrôles sont bons, et si le produit de l'opération de vérification est «oui» l'utilisateur est accepté.

3.3.3 Variante

Notons qu'une fois que l'utilisateur et l'opérateur de réseau ont utilisé le mécanisme ci-dessus, ce mécanisme peut être simplifié en remplaçant le certificat CERT par l'identité TMUI (en supposant que l'opérateur de réseau occulte la clé de vérification publique de l'utilisateur et l'identité correspondante TMUI). Cela permettra d'économiser de la largeur de bande et une opération de vérification à l'opérateur de réseau.

3.4 Évaluation

Le mécanisme a les caractéristiques significatives suivantes.

3.4.1 Fourniture de services de sécurité

Le mécanisme de sécurité fournit les services d'authentification pour lesquels il a été conçu.

Il existe un certain nombre d'algorithmes de chiffrement à clé publique et à signature numérique adaptés.

3.4.2 Préfixes – communications

Dans ce mécanisme, un seul message doit être envoyé. C'est le minimum requis pour l'authentification unilatérale; le service de confidentialité de l'identité est assuré sans qu'il soit nécessaire d'envoyer d'autres messages. Tous les messages seront relativement longs; le champ SIG de la chaîne déchiffrée peut contenir entre 512 et 1 024 bits et l'opération de chiffrement peut allonger encore le message.

3.4.3 Préfixes – administration

Dans ce mécanisme, les entités sont tenues de mettre en mémoire des questions aléatoires pendant de brèves périodes de temps. Les identités temporaires devront elles aussi être mises en mémoire par les utilisateurs et les opérateurs de réseau. Le fournisseur de services n'est pas nécessairement concerné sauf pour la délivrance de certificats à de nouveaux utilisateurs.

La taille des clés pour les algorithmes asymétriques est en général assez importante (1024 bits ou plus) comparée à celle des clés pour un algorithme classique (64 à 128 bits).

Les utilisateurs devront mettre en mémoire des clés de chiffrement publiques de tous les opérateurs de réseau avec lesquels ils pourraient avoir besoin de communiquer. Les clés pourraient être distribuées à un utilisateur par le fournisseur de services.

Les opérateurs de réseau doivent mettre en mémoire des clés de vérification publiques de tous les fournisseurs de services avec lesquels ils ont conclu un accord de fourniture de services.

Comme on l'a déjà indiqué, il faut que les utilisateurs, les opérateurs de réseau et les fournisseurs de services aient accès à des horloges synchronisées.

3.4.4 Préfixes – traitement et autre matériel

Les calculs pour les opérations de signature et de vérification peuvent être relativement complexes; cette complexité dépendra de l'algorithme et de la taille des clés utilisées. De même, les opérations de chiffrement et de déchiffrement de clés publiques peuvent être relativement complexes.

3.4.5 Respect des normes internationales

Le mécanisme peut être conforme à la Norme ISO/CEI 9798-3: 1993 (à condition que les éléments du message soient assemblés dans le bon ordre); on ne sait pas si la norme autorise le chiffrement des échanges d'authentification (il s'agit d'une question d'interprétation).

3.4.6 Limitation d'utilisation

Le mécanisme utilise un algorithme à signature numérique et un algorithme de chiffrement à clé publique. Étant donné qu'il intègre une fonction de chiffrement, la mobilité transfrontière de l'équipement mettant en œuvre ce mécanisme sera vraisemblablement facilitée. Le mécanisme lui-même ne fait l'objet d'aucune restriction en matière de brevets, même si certains algorithmes à signature numérique et certains algorithmes de chiffrement à clé publique sont couverts par des brevets.