Groupe de travail Réseau
**Request for Comments: 4442**
Catégorie : Sur la voire de la normalisation
Traduction Claude Brière de L'Isle

S. Fries, Siemens
H. Tschofenig, Siemens
mars 2006

# Amorçage de l'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA)



**Résumé**
TESLA, le protocole d'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA, *Timed Efficient Stream Loss-tolerant Authentication*) assure l'authentification de la source dans les scénarios de diffusion groupée. TESLA est un protocole efficace avec de faible redondance de communication et de calcul qui s'adapte à un grand nombre de receveurs et aussi tolère les pertes de paquets. TESLA se fonde sur une synchronisation lâche entre l'envoyeur et les receveurs. L'authentification de la source est réalisée dans TESLA en utilisant un chaînage de codes d'authentification de message (MAC, *Message Authentication Code*). L'utilisation de TESLA dans le protocole de transport sûr en temps réel (SRTP, *Secure Real-time Transport Protocol*) a été publiée, ciblant l'authentification de diffusion groupée dans des scénarios où SRTP est appliqué pour protéger des données multimédia. Cette solution suppose que les paramètres de TESLA sont disponibles par des mécanismes hors bande.

Le présent document spécifie les charges utiles pour le protocole de chiffrement Internet multimédia (MIKEY, *Multimedia Internet Keying*) pour l'amorçage de TESLA pour l'authentification de la source de communications de groupe sûres en utilisant SRTP. TESLA peut être amorcé en utilisant une des approches de gestion de clé de MIKEY, par exemple, en utilisant un message MIKEY signé numériquement envoyé via envoi individuel, diffusion, ou diffusion groupée.

## Table des matières

1. Introduction....2
2. Terminologie....2
3. Généralités sur les paramètres de TESLA....3
4. Codage des paramètres dans MIKEY....3
4.1. Charge utile de politique de sécurité (SP)....3
4.2 Politique de TESLA....4
4.3 Synchronisation....5
4.4 Transport des données de clés dans la charge utile Extension générale de MIKEY....5
5. Considérations sur la sécurité....6
5.1 Attaque par interposition....6
5.2 Attaque en dégradation....6
5.3 Attaque de déni de service....7
5.4 Attaque en répétition....7
5.5 Analyse de trafic....7
6. Considérations relatives à l'IANA....7
7. Remerciements....8
8. Références....8
8.1 Références normatives....8
8.2 Références pour information....9
Adresse des auteurs....9
Déclaration complète de droits de reproduction....9

## 1. Introduction

Dans de nombreux scénarios de communication en envoi individuel, en diffusion et en diffusion groupée, il est nécessaire de garantir qu'un message reçu a été envoyé par une source dédiée et n'a pas été altéré dans le transit. Dans une communication en envoi individuel, il existe couramment une association de sécurité entre les pairs qui permet la validation de l'intégrité du message et de l'origine des données. L'approche est différente dans les communications fondées sur le groupe, car une clé y est normalement partagée entre les membres d'un groupe et donc ne peut pas être utilisée pour l'authentification de l'origine des données. Comme dans certaines applications une identification dédiée de l'envoyeur est requise, il existe l'exigence de prendre en charge l'authentification de l'origine aussi dans les scénarios de diffusion groupée. Une des méthodes pour prendre cela en charge est TESLA [RFC4082]. TESLA fournit l'authentification de la source dans les scénarios de diffusion groupée en utilisant le chaînage de MAC. Il se fonde sur la synchronisation lâche entre l'envoyeur et les receveurs.

La [RFC4383] décrit les extensions à SRTP [RFC3711] afin de prendre en charge TESLA [RFC4082] pour l'authentification de source dans les scénarios de diffusion groupée. SRTP a besoin d'un contexte cryptographique dédié pour décrire les paramètres de sécurité et la politique de sécurité par session multimédia à protéger. Ce contexte cryptographique a besoin d'être amélioré avec un ensemble de paramètres TESLA. Il est nécessaire de fournir ces paramètres avant que commence la session de diffusion groupée réelle. La [RFC4383] ne traite pas de l'amorçage pour ces paramètres.

Le présent document détaille l'amorçage des paramètres TESLA en termes de distribution de paramètres pour la politique de TESLA ainsi que de clé initiale, en utilisant le protocole de chiffrement Internet multimédia (MIKEY, *Multimedia Internet Keying*) [RFC3830]. MIKEY définit un cadre d'authentification et de gestion de clé qui peut être utilisé pour des applications en temps réel (à la fois pour des communication d'homologue à homologue et des communications de groupe). En particulier, la [RFC3830] est définie d'une façon qui est destinée à prendre en charge SRTP en premier lieu, mais est ouverte aux améliorations pour être aussi utilisée pour d'autres objets. Suivant la description de la [RFC3830], MIKEY est tourné vers les communications en point à point aussi bien que de groupe. Dans le contexte de la communication de groupe, une entité administrative peut distribuer les clés de session aux entités associées qui participent à la session de communication.

Ce scénario est aussi applicable à TESLA où une entité peut fournir des informations à de nombreuses autres de façon à assurer l'intégrité des informations communiquées. La combinaison de MIKEY et TESLA prend en charge cette approche fondée sur le groupe en utilisant le cadre de MIKEY pour distribuer les informations de paramètres de TESLA aux entités impliquées. Noter que ce document se concentre seulement sur la distribution des paramètres, et non sur leur génération.

MIKEY [RFC3830] lui-même décrit trois protocoles d'authentification et d'échange de clés (chiffrement à clés symétriques, chiffrement à clé publique, et Diffie-Hellman signé). Les extensions aux méthodes d'échange de clé MIKEY ont été définies. Une quatrième méthode de distribution de clés est fournie par la [RFC4650] et décrit un accord de clés Diffie-Hellman à protection symétrique. Une autre option a été proposée dans la [RFC4738] qui décrit une variante améliorée d'échange asymétrique, qui prend aussi en charge un échange de certificat dans la bande. Tous les différents schémas de gestion de clé mentionnés ci-dessus peuvent être utilisés pour fournir les paramètres TESLA. Les paramètres TESLA dont l'échange est exigé sont déjà décrits dans la [RFC4383], tandis que le présent document décrit leur transport avec MIKEY.

Les exigences de sécurité suivantes ont été formulées pour l'échange des paramètres TESLA :
- L'authentification et la protection de l'intégrité DOIVENT être fournies lors de l'envoi des paramètres de TESLA, en particulier pour la clé initiale.
- La confidentialité PEUT être fournie pour les paramètres TESLA.

Ces exigences de sécurité s'appliquent seulement à la procédure d'amorçage de TESLA. Les exigences de sécurité pour les applications qui utilisent TESLA sortent du domaine d'application du présent document. Les aspects de sécurité qui se rapportent à TESLA lui-même sont décrits dans la [RFC4082], et les questions de sécurité pour l'utilisation de TESLA pour SRTP sont couvertes dans la [RFC4383].

Il est important de noter que le présent document est un élément d'une solution complète. En supposant que le trafic sur le support doive être sécurisé en utilisant TESLA comme décrit dans la [RFC4383], alors (a) le matériel de chiffrement et (b) les paramètres pour TESLA sont nécessaires. Le présent document contribue aux paramètres et aux méthodes d'authentification utilisées dans MIKEY pour fournir le matériel de chiffrement. L'échange des paramètres pour TESLA doit aussi être sécurisé contre l'altération. Cette protection est aussi fournie par MIKEY.

## 2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

## 3. Généralités sur les paramètres de TESLA

Selon la [RFC4383], un certain nombre de paramètres dépendants de la transformation doivent être fournis pour un fonctionnement approprié de TESLA. La liste complète des paramètres se trouve au paragraphe 4.3 de la [RFC4383]. Noter que le paramètre 10 de la [RFC4383], qui décrit le décalage de l'horloge du receveur par rapport à celle de l'envoyeur, est omis dans le présent document car il peut être calculé.

MIKEY exige déjà des horloges synchronisées, qui assurent aussi la synchronisation pour TESLA. De plus, le paragraphe 4.3 déclare une option d'utilisation de MIKEY pour la détermination de la dérive d'horloge entre l'envoyeur et le receveur. Donc, ce paramètre n'a pas besoin d'être transmis directement dans MIKEY.

Les informations entre parenthèses donnent les valeurs par défaut comme spécifié au paragraphe 6.2 de la [RFC4383].

1. Un identifiant pour la PRF (PRF TESLA) qui met en œuvre la fonction unidirectionnelle F(x) dans TESLA (pour déduire les clés dans la chaîne) et la fonction unidirectionnelle F'(x) dans TESLA (pour déduire les clés pour le MAC TESLA, à partir des clés dans la chaîne) par exemple, pour indiquer la fonction de hachage chiffré (par défaut HMAC-SHA1).

2. Un entier non négatif, déterminant la longueur du résultat F, c'est-à-dire, la longueur des clés dans la chaîne, qui est aussi la clé divulguée dans un paquet SRTP si TESLA est utilisé dans le contexte SRTP (160 bits par défaut).

3. Un entier non négatif, déterminant la longueur du résultat de F', c'est-à-dire, la longueur de la clé pour le MAC TESLA (160 bits par défaut).

4. Un identifiant pour le MAC TESLA qui accepte le résultat de F'(x) comme sa clé, par exemple, pour indiquer une fonction de hachage chiffré (par défaut HMAC-SHA1).

5. Un entier non négatif, déterminant la longueur du résultat du MAC TESLA (80 bits par défaut).

6. Le début de la session pour laquelle une clé sera appliquée.

7. La durée de l'intervalle (en millisecondes) pour lequel une clé dédiée sera utilisée.

8. Le délai de divulgation de clé (en nombre d'intervalles) caractérise la période après laquelle la clé sera envoyée aux entités impliquées (par exemple, au titre de paquets SRTP).

9. Un entier non négatif, déterminant la longueur de la chaîne de clés, qui est déterminée sur la base de la durée attendue du flux.

10. La clé initiale de la chaîne à laquelle l'envoyeur s'est engagé.

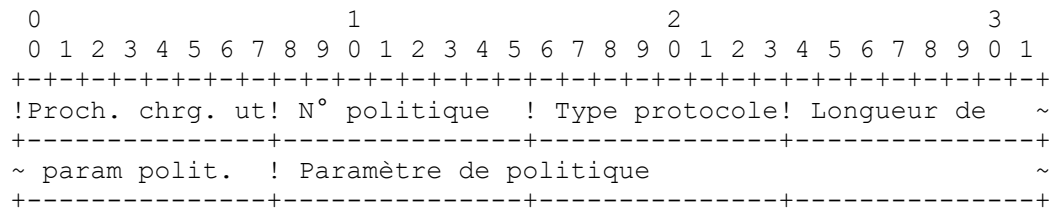
## 4. Codage des paramètres dans MIKEY

Comme mentionné à la Section 3, les paramètres TESLA doivent être transportés avant de commencer réellement une session. MIKEY définit actuellement seulement une charge utile pour transporter la politique SRTP (voir au paragraphe 6.10 de la [RFC3830]). Cette Section décrit les améliorations de MIKEY pour permettre le transport d'une politique TESLA et de la clé initiale TESLA.

### 4.1. Charge utile de politique de sécurité (SP)

La charge utile Politique de sécurité définit un ensemble de politiques qui s'appliquent à un protocole de sécurité

spécifique. La définition s'appuie sur le définition de charge utile de politique de sécurité de la [RFC3830].




* Prochaine charge utile (8 bits) : identifie la charge utile ajoutée après cette charge utile. Voir les détails au paragraphe 6.1 de la [RFC3830].

* N° de politique (8 bits) : chaque charge utile Politique de sécurité doit recevoir un numéro distinct pour la session MIKEY en cours de la part de l'homologue local. Ce numéro est utilisé pour transposer une session cryptographique en une politique spécifique (voir aussi le paragraphe 6.1.1 de la [RFC3830]).

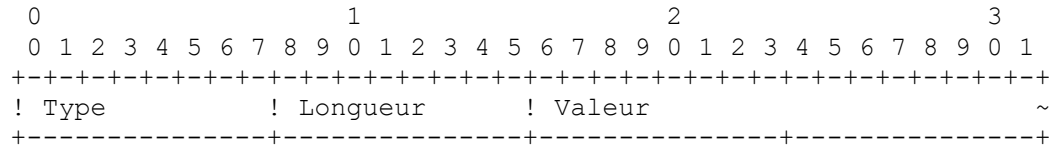
* Type de protocole (8 bits) : cette valeur définit le protocole de sécurité. Une seconde valeur doit être définie comme montré ci-dessous : (MIKEY définit déjà la valeur 0.)

| **Type de protocole** | **Valeur** |
|---|---|
| SRTP | 0 |
| TESLA | 1 |

* Longueur de paramètre de politique (16 bits) : ce champ définit la longueur totale des paramètres de politique pour le protocole de sécurité choisi.

* Paramètre de politique (longueur variable) : ce champ définit la politique pour le protocole de sécurité spécifique.

La partie Paramètre de politique est constituée d'un ensemble de charges utiles Type/Longueur/Valeur (TLV). Pour chaque protocole de sécurité, un ensemble de paires type/valeur possibles peut être négocié comme défini.




* Type (8 bits) : spécifie le type du paramètre.

* Longueur (8 bits) : spécifie la longueur du champ Valeur (en octets).

* Valeur (longueur variable) : spécifie la valeur du paramètre.

### 4.2 Politique de TESLA

Cette politique spécifie les paramètres pour TESLA. Les types/valeurs qui peuvent être négociés sont définis par le tableau qui suit. Les valeurs par défaut sont tirées de la [RFC4383], mais d'autres valeurs peuvent aussi être utilisées :

| **Type** | **Signification** | **Valeurs possibles** |
|---|---|---|
| 1 | Identifiant de PRF pour f et f', réalisant F(x) et F'(x) | voir ci-dessous |
| 2 | Longueur du résultat de la PRF f | 160 |
| 3 | Identifiant pour le MAC TESLA | voir ci-dessous |
| 4 | Longueur du résultat du MAC TESLA | 80 (tronqué) |
| 5 | Début de session | en octets |
| 6 | Durée d'intervalle (en ms) | en octets |
| 7 | Délai de divulgation de clé | en octets |
| 8 | Longueur de chaîne de clés (nombre d'intervalles) | en octets |
| 9 | Horodatage local du receveur du support | voir ci-dessous |

Les valeurs de temps déclarées dans les points 5 et 9 DEVRONT être transportées en format NTP-UTC, qui est une des

trois options décrites au paragraphe 6.6 de la [RFC3830]. Une valeur d'entier de quatre octets pour l'élément de politique 6 et une valeur d'entier de deux octets pour l'élément de politique 7 sont RECOMMANDÉES, portant une durée d'intervalle et un délai de divulgation de clé. Le type de politique 9 déclaré ci-dessus est facultatif et DEVRAIT être utilisé si la synchronisation décrite au paragraphe 4.3, point deux, est utilisée. Autrement, il DEVRAIT être omis.

Pour la PRF réalisant F(x) et F'(x), une longueur d'un octet est suffisante. Les valeurs possibles actuellement définies sont :

| **PRF TESLA F(x), F'(x)** | **Valeur** |
|---|---|
| HMAC-SHA1 | 0 |

Pour le MAC TESLA, une longueur d'un octet est suffisante. Les valeurs possibles actuellement définies sont :

| **MAC TESLA** | **Valeur** |
|---|---|
| HMAC-SHA1 | 0 |

### 4.3 Synchronisation

MIKEY tout comme TESLA exige la synchronisation des homologues communicants. MIKEY exige la synchronisation pour fournir la protection contre la répétition fondée sur l'horodatage pour les protocoles d'authentification sur un aller-retour et d'échange de clés. TESLA, par ailleurs, a besoin de ces informations pour déterminer la dérive d'horloge entre les envoyeurs et les receveurs afin de libérer de façon appropriée la clé divulguée. Deux solutions sont disponibles pour la synchronisation :

1. Synchronisation hors bande en utilisant NTP [RFC1305]. Cette approche est déjà recommandée dans la [RFC3830]. L'avantage de cette approche est l'option d'utiliser les variantes de gestion de clé MIKEY qui s'effectuent sur un demi aller-retour. L'inconvénient est l'utilisation d'un protocole supplémentaire.

2. La [RFC4082] décrit aussi une possible synchronisation dans la bande dans son paragraphe 3.3.1. Cette approche est résumée ici dans le contexte de MIKEY. Noter qu'ici la charge utile de politique TESLA réelle est transmise au titre du message de réponse MIKEY.

   * Le receveur des données, qui serait l'initiateur MIKEY, règle le paramètre d'heure locale t_r et l'envoie au titre de la charge utile Horodatage comme décrit dans la [RFC3830]. Cette valeur t_r doit être mémorisée en local.

   * À réception du message initiateur MIKEY, l'envoyeur des données répond avec le message répondant MIKEY, réglant l'horodatage local chez le receveur des données (paramètre 11) à la valeur t_r reçue dans le message initiateur MIKEY, et règle son heure locale comme une valeur UTC de 64 bits t_s dans la charge utile Horodatage comme décrit dans la [RFC3830].

   Message initiateur MIKEY
   [paramètre MIKEY incluant l'horodatage local (t_r)]
   ------------------>

   Message répondant MIKEY
   [paramètre MIKEY incluant l'horodatage local (t_s), charge utile Politique TESLA, horodatage local reçu t_r]
   <------------------

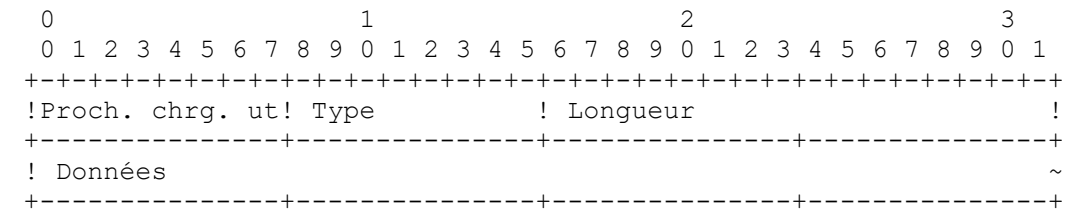
   * À réception du message répondant MIKEY le receveur des données règle D_t = t_s - t_r + S, où S est une limite estimée de la dérive d'horloge sur la durée de la session.

   Cette approche présente l'avantage de ne pas exiger de protocole de synchronisation supplémentaire. L'inconvénient est la nécessité d'effectuer une prise de contact MIKEY complète, pour permettre un transport correct de paramètres. De plus, cette approche dépend de la direction, car elle ne peut être appliquée que si le receveur du support est aussi l'initiateur MIKEY.

La synchronisation hors bande utilisant NTP (c'est-à-dire, la solution 1) est l'approche RECOMMANDÉE pour la synchronisation d'horloge. Dans les scénarios où le receveur du support est aussi l'initiateur MIKEY, porter les informations d'horodatage dans MIKEY (c'est-à-dire, la solution 2) PEUT être utilisé pour permettre la détermination dans la bande de la dérive d'horloge entre envoyeur et receveur.

### 4.4 Transport des données de clés dans la charge utile Extension générale de MIKEY

La charge utile Extensions générales a été définie pour permettre des extensions à MIKEY sans avoir besoin de définir à chaque fois une charge utile complètement nouvelle. Cette charge utile peut être utilisée dans tout message MIKEY et fait partie de la partie de données authentifiée/signée.




* Prochaine charge utile (8 bits) : identifie la charge utile qui suit cette charge utile.

* Type (8 bits) : identifie le type de la charge utile générale. MIKEY définit déjà les valeurs 0 et 1. Le présent document introduit une nouvelle valeur (2).

| Type | Valeur | Commentaires |
|---|---|---|
| Vendor ID | 0 | Chaîne d'octets spécifique du fabricant |
| SDP ID | 1 | Liste des identifiants de gestion de clés SDP |
| TESLA I-Key | 2 | Clé initiale TESLA |

* Longueur (16 bits) : longueur en octets du champ Données.

* Données (longueur variable) : données de charge utile générale.

## 5. Considérations sur la sécurité

Les propriétés de sécurité des données multi supports dans un environnement de diffusion groupée dépendent d'un certain nombre de blocs de construction.

SRTP-TESLA [RFC4383] décrit les extensions pour SRTP [RFC3711] afin de prendre en charge TESLA [RFC4082] pour l'authentification de la source dans les scénarios de diffusion groupée. À ce titre, les considérations sur la sécurité décrites dans TESLA (voir [PCST] et la [RFC4082]) la transposition SRTP de TESLA [RFC4383], et SRTP [RFC3711] lui-même sont pertinentes dans ce contexte.

De plus, comme ce document détaille l'amorçage de TESLA en utilisant le protocole de chiffrement Internet multimédia (MIKEY, *Multimedia Internet Keying)* [RFC3830] les considérations sur la sécurité de MIKEY sont applicables au présent document.

En résumé, pour qu'une application multimédia prenne en charge TESLA, les interactions de protocole suivantes (en relation avec le présent document) sont nécessaires :
- o MIKEY [RFC3830] est exécuté entre les entités désirées pour effectuer l'authentification et une distribution sécurisée du matériel de chiffrement. Pour utiliser ultérieurement TESLA, les paramètres décrits dans le présent document sont distribués en utilisant MIKEY. MIKEY lui-même utilise un autre protocole pour le transport de paramètres, à savoir le protocole de description de session (SDP, *Session Description Protocol*) [RFC2327]. SDP peut encore être utilisé au sein du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261] pour établir une session entre les entités désirées.
- o Après que les algorithmes, les paramètres, et les clés de session sont disponibles aux entités respectives de communication, la protection du trafic de données via SRTP-TESLA [RFC4383] peut être utilisée. SRTP-TESLA applique lui-même TESLA au protocole SRTP, et à ce titre les lignes directrices sur le traitement de TESLA doivent être suivies.

### 5.1 Attaque par interposition

Menace : L'échange des paramètres et algorithmes relatifs à la sécurité sans authentification mutuelle des deux homologues peut permettre à un adversaire d'effectuer une attaque par interposition. Les mécanismes décrits dans le présent document ne fournissent pas eux-même une telle authentification et protection de l'intégrité.

Contre mesures : Dans tout ce document, on a supposé que l'échange de paramètres est sécurisé en utilisant un autre protocole, c'est-à-dire que l'échange de paramètres et les algorithmes font partie d'un protocole d'authentification et d'échange de clés (à savoir MIKEY). L'authentification de la source des communications de groupe et de diffusion groupée ne peut pas être fournie pour le trafic de données si l'échange de signalisation préalable n'a pas fourni de facilités pour authentifier la source. Utiliser un protocole d'authentification qui ne donne pas des clés de session au titre d'un échange de protocole réussi va rendre impossible de déduire les paramètres requis par TESLA. MIKEY fournit l'établissement des clés de session. De plus, l'échange des paramètres et algorithmes DOIT être authentifié et leur intégrité protégée. La protection de l'échange de paramètres doit fournit le même niveau de sécurité ou un niveau supérieur.

### 5.2 Attaque en dégradation

Menace : L'échange des paramètres et algorithmes relatifs à la sécurité est toujours soumis à des attaques en dégradation par lesquelles un adversaire modifie certains (ou tous) des paramètres fournis. Par exemple, certains paramètres exigent que soit mentionné un algorithme de hachage pris en charge. Pour monter une attaque, l'adversaire doit modifier la liste des algorithmes choisis et retenir le plus faible.

Contre mesures : L'amorçage de paramètre TESLA DOIT être protégé en intégrité pour empêcher la modification des paramètres et de leurs valeurs. De plus, comme des paramètres non modifiés provenant d'une source inconnue ne sont d'aucune utilité, l'authentification DOIT être assurée. Cette fonctionnalité n'est pas fournie par les mécanismes décrits dans le présent document. À la place, les capacités du protocole sous-jacent d'authentification et d'échange de clé (MIKEY) sont réutilisées à cette fin.

### 5.3 Attaque de déni de service

Menace : un adversaire peut vouloir modifier les paramètres échangés entre les entités communicantes afin d'établir des informations d'état différentes dans les entités respectives de communication. Par exemple, un adversaire peut vouloir modifier le délai de divulgation de clé ou la durée de l'intervalle afin de perturber la communication à un état ultérieur car l'algorithme de TESLA suppose que les entités de communication participantes connaissent le même ensemble de paramètres.

Contre mesures : les paramètres échangés et les paramètres et algorithmes DOIVENT être protégés en intégrité pour permettre au receveur de détecter si un adversaire a tenté de modifier les informations échangées. Les algorithmes d'authentification et d'échange de clés fournis par MIKEY offrent cette protection.

### 5.4 Attaque en répétition

Menace : un adversaire qui est capable d'espionner un ou plusieurs échanges de protocole (échanges MIKEY avec les paramètres décrits dans le présent document) peut être capable de répéter les charges utiles dans un échange de protocole ultérieur. Si les receveurs acceptent les paramètres et algorithmes (ou même les messages qui portent ces charges utiles) alors une attaque de déni de service, de dégradation, ou d'interposition peut en être la conséquence (selon l'ensemble entier d'attributs et messages répétés).

Contre mesures : afin d'empêcher les attaques en répétition, une garantie de fraîcheur DOIT être fournie. À ce titre l'échange de messages d'amorçage TESLA doit être unique et frais, et le protocole correspondant d'authentification et d'échange de clés DOIT fournir les mêmes propriétés. En fait, il est essentiel de déduire une clé de session unique et fraîche au titre du protocole d'authentification et d'échange de clés qui DOIT être lié à la session de protocole. Cela inclut les paramètres échangés.

### 5.5 Analyse de trafic

Menace : un adversaire peut être capable d'apprendre les paramètres et algorithmes si il est situé sur le chemin de signalisation. Ces informations peuvent ensuite être utilisées pour monter des attaques contre la communication multimédia de bout en bout. Dans certains environnements de haute sécurité et militaires, il peut même être souhaitable de ne pas révéler d'informations sur les paramètres utilisés pour rendre plus difficile de lancer une attaque.

Contre mesures : la protection de la confidentialité peut être fournie par un sous ensemble des protocoles disponibles d'authentification et d'échange de clé de MIKEY, à savoir, ceux qui fournissent le chiffrement à clé publique et le chiffrement à clé symétrique. La clé de hachage initiale, qui est aussi un des paramètres d'amorçage de TESLA,

n'exige pas de protection de la confidentialité du fait des propriétés d'une chaîne hachée.

## 6. Considérations relatives à l'IANA

Le présent document demande l'enregistrement par l'IANA des attributs suivants. Les registres sont fournis par MIKEY [RFC3830].

Type de protocole : cet attribut spécifie le type de protocole de sécurité comme décrit au paragraphe 4.1.

Type : identifie le type de la charge utile générale. La charge utile Extensions générale a été définie pour permettre des extensions à MIKEY sans avoir besoin de définir une charge utile complètement nouvelle à chaque fois. Le paragraphe 4.4 décrit cet attribut en détail.

Suivant les politiques mentionnées dans la [RFC3830], les valeurs dans la gamme de 0 à 240 (inclus) pour les attributs ci-dessus sont alloués après revue d'expert par le groupe de travail MSEC ou son successeur désigné. Les valeurs dans la gamme de 241 à 255 sont réservées pour utilisation privée.

L'IANA a ajouté les attributs suivants et leurs valeurs respectives à un registre existant créé dans la [RFC3830] :

Type de protocole :

| **Type de protocole** | **Valeur** | **Description** |
|---|---|---|
| TESLA | 1 | TESLA comme protocole de sécurité |

La valeur 1 pour le Type de protocole doit être ajoutée au registre "Prot type" créé par la [RFC3830].

Type :

| **Type** | **Valeur** | **Description** |
|---|---|---|
| TESLA I-Key | 2 | Clé initiale TESLA |

La valeur 2 pour le "Type" doit être ajoutée au registre "Type" créé par la [RFC3830]. Les valeurs 0 et 1 sont déjà enregistrées dans la [RFC3830].

Aussi, l'IANA a créé deux nouveaux registres :

TESLA-PRF : fonctions pseudo aléatoires (PRF) utilisées dans la politique TESLA : cet attribut spécifie les valeurs pour les fonctions pseudo aléatoires utilisées dans la politique TESLA (voir au paragraphe 4.2).

TESLA-MAC : fonction de MAC utilisée dans TESLA : cet attribut spécifie les valeurs des fonctions pseudo aléatoires utilisées dans la politique TESLA (voir au paragraphe 4.2).

Suivant les politiques mentionnées dans la [RFC2434], les valeurs pour les registres TESLA-PRF et TESLA-MAC dans la gamme de 0 à 240 (inclus) pour les attributs ci-dessus sont allouées après revue d'expert par le groupe de travail MSEC ou son successeur désigné. Les valeurs dans la gamme de 241 à 255 sont réservées pour utilisation privée.

L'IANA a ajouté les valeurs suivantes aux registres TESLA-PRF et TESLA-MAC :

TESLA-PRF :

| **Fonction PRF** | **Valeur** |
|---|---|
| HMAC-SHA1 | 0 |

TESLA-MAC :

| **Fonction MAC** | **Valeur** |
|---|---|
| HMAC-SHA1 | 0 |

## 7. Remerciements

Les auteurs tiennent à remercier Mark Baugher et Ran Canetti pour les discussions dans le contexte de la synchronisation. De plus, nous souhaitons remercier Lakshminath Dondeti, Russ Housley, et Allison Mankin de leur relecture du document

et de leurs conseils.

## 8. Références

### 8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC3830] J. Arkko et autres, "MIKEY : Gestion de clé multimédia pour l'Internet", août 2004. (*MàJ par* RFC4738) *(P.S.)*

[RFC4082] A. Perrig et autres, "Authentification de flux tolérante aux pertes en temps efficace (TESLA) : Introduction à la transformation d'authentification de source de diffusion groupée", juin 2005. *(Information)*

[RFC4383] M. Baugher, E. Carrara, "Utilisation de l'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA) dans le protocole de transport en temps réel sécurisé (SRTP)", février 2006. *(P.S.)*

### 8.2 Références pour information

[PCST] Perrig, A., Canetti, R., Song, D., et D. Tygar, "Efficient et Secure Source Authentication for Multicast", dans Proc. of Network et Distributed System Security Symposium NDSS 2001, pp. 35-46, 2001.

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars992. *(Remplacée par* RFC5905)

[RFC2327] M. Handley et V. Jacobson, "SDP : Protocole de description de session", avril 1998. *(Obsolète; voir* RFC4566)

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3711] M. Baugher et autres, "Protocole de transport sécurisé en temps réel (SRTP)", mars 2004. *(P.S.)*

[RFC4650] M. Euchner, "Diffie-Hellman authentifié en HMAC pour le protocole de chiffrement Internet multimédia (MIKEY)", septembre 2006. *(P.S.)*

[RFC4738] D. Ignjatic et autres, "MIKEY-RSA-R : un mode supplémentaire de distribution de clés dans le chiffrement Internet multimédia (MIKEY)", novembre 2006. (*MàJ* RFC3830) *(P.S.)*

## Adresse des auteurs

Steffen Fries
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany
mél : steffen.fries@siemens.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany
mél : Hannes.Tschofenig@siemens.com

## Déclaration complète de droits de reproduction

**Remerciement**
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA, *IETF Administrative Support Activity*).