Groupe de travail Réseau
Request for Comments : 4474
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Peterson, NeuStar
C. Jennings, Cisco Systems
août 2006

Améliorations de la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright
Copyright (C) The Internet Society (2006).

Résumé
Les mécanismes de sécurité existants dans le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) sont inadéquats pour assurer cryptographiquement l'identité des utilisateurs finaux qui génèrent des demandes SIP, en particulier dans un contexte inter domaines. Le présent document définit un mécanisme pour identifier de façon sûre les générateurs de messages SIP. Il le fait en définissant deux nouveaux champs d'en-tête SIP, Identity, pour porter une signature utilisée pour valider l'identité, et Identity-Info, pour porter une référence au certificat du signataire.

Table des matières

1. Introduction

Le présent document apporte des améliorations aux mécanismes existants pour la gestion de l'identité authentifiée dans le protocole d'initialisation de session (SIP) [RFC3261]. Une identité, pour les besoins du présent document, est définie comme un URI SIP, généralement l'adresse d'enregistrement (AoR, A*ddress of Reccord*) canonique employée pour joindre un utilisateur (comme "sip:alice@atlanta.exemple.com").

La RFC 3261 stipule plusieurs endroits au sein d'une demande SIP où un utilisateur peut exprimer une identité pour lui-même, notamment le champ d'en-tête From rempli par l'utilisateur. Cependant, le receveur d'une demande SIP n'a aucun moyen de vérifier que le champ d'en-tête From a été rempli de façon appropriée, en l'absence d'un mécanisme d'authentification cryptographique.

La RFC 3261 spécifie un certain nombre de mécanismes de sécurité qui peuvent être employés par les agents d'utilisateur SIP (UA), incluant le résumé *(digest)*, la sécurité de la couche Transport (TLS, *Transport Layer Security*), et S/MIME (les mises en œuvre peuvent aussi prendre en charge d'autres schémas de sécurité). Cependant, peu d'agents d'utilisateur SIP prennent aujourd'hui en charge les certificats d'utilisateur final nécessaires pour s'authentifier (via S/MIME, par exemple), et de plus l'authentification par résumé est limitée par le fait que l'origine et la destination doivent partager un secret pré arrangé. Il est souhaitable que les agents d'utilisateur SIP soient capables d'envoyer des demandes aux destinations avec lesquelles elles n'ont pas d'association antérieure -- tout comme dans le réseau téléphonique d'aujourd'hui, on peut recevoir un appel de quelqu'un avec qui on a pas eu de contact préalable, et avoir quand même une assurance raisonnable que l'identifiant d'appelant affiché de la personne est fondé. Une approche cryptographique, comme celle décrite dans le présent document, peut probablement fournir une assurance de l'identité beaucoup plus forte et moins susceptible d'être usurpée que ce que le réseau de téléphone fournit aujourd'hui.

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] et indiquent les niveaux d'exigences pour les mises en œuvre conformes.

3. Fondements

L'usage de nombreuses applications et services SIP est gouverné par des politiques d'autorisation. Ces politiques peuvent être automatisées, ou elles peuvent être appliquées manuellement par les hommes. Un exemple de ces dernières serait celui d'une application de téléphone Internet qui affiche l'identifiant d'appelant *(Caller-ID)* d'un appelant, qu'un humain peut voir avant de répondre à l'appel. Un exemple des premières serait un service de présence qui compare l'identité d'abonnés potentiels à une liste avant de déterminer si il devrait accepter ou rejeter la demande d'abonnement. Dans ces deux cas, des attaquants pourraient tenter de circonvenir ces politiques d'autorisation par une usurpation d'identité. Comme principal identifiant de l'envoyeur d'une demande SIP, le champ d'en-tête From, peut être rempli de façon arbitraire par le contrôleur d'un agent d'utilisateur, et donc l'usurpation d'identité est très simple aujourd'hui. Le mécanisme décrit dans le présent document aspire à fournir un système d'identité fort pour SIP dans lequel les politiques d'autorisation ne peuvent pas être circonvenues par l'usurpation d'identité.

Tous les agents d'utilisateur conformes à la RFC 3261 prennent en charge l'authentification par résumé, qui utilise un secret partagé, comme moyen pour s'authentifier auprès d'un registraire SIP. L'enregistrement permet à un agent d'utilisateur d'exprimer qu'il est une entité appropriée à laquelle les demandes devraient être envoyées pour un certain URI d'AoR SIP (par exemple, "sip:alice@atlanta.exemple.com").

Par la définition de l'identité utilisée dans le présent document, l'enregistrement est une preuve de l'identité de l'utilisateur donnée à un registraire. Cependant, les accréditifs avec lesquels un agent d'utilisateur prouve son identité à un registraire ne

peuvent pas être validés par juste n'importe quel agent d'utilisateur ou serveur mandataire – ces accréditifs sont partagés seulement entre l'agent d'utilisateur et son administrateur de domaine. Donc, ce secret partagé n'aide pas immédiatement un utilisateur à authentifier une large gamme de receveurs. Les receveurs exigent un moyen pour déterminer si l'identité de "l'adresse de retour" d'une demande non REGISTER (c'est-à-dire, la valeur du champ d'en-tête From) a été légitimement affirmée.

L'URI d'AoR utilisé pour l'enregistrement est aussi l'URI avec lequel un UA remplit habituellement le champ d'en-tête From des demandes afin de fournir une identité d'adresse de retour aux receveurs. Du point de vue de l'autorisation, si on peut prouver qu'on est éligible à l'enregistrement dans un domaine sous une AoR particulière, on peut prouver qu'on peut légitimement recevoir des demandes pour cette AoR, et en conséquence, quand on place cette AoR dans le champ d'en-tête From d'une demande SIP autre qu'un enregistrement (comme un INVITE) on fournit une adresse de retour où on peut légitimement être joint. En d'autres termes, si on est autorisé à recevoir des demandes pour cette adresse de retour, il s'ensuit logiquement qu'on est aussi autorisé à affirmer cette adresse de retour dans le champ d'en-tête From. Ceci est bien sûr seulement une manière dont un domaine peut déterminer comment un utilisateur particulier est autorisé à remplir le champ d'en-tête From ; par ailleurs, pour d'autres sortes d'URI dans le From (comme les URI anonymes) d'autres politiques d'autorisation vont s'appliquer.

Idéalement, les agents d'utilisateur SIP devraient avoir un moyen de prouver aux receveurs de demandes SIP que leur domaine local les a authentifié et a autorisé le remplissage du champ d'en-tête From. Le présent document propose une architecture d'authentification médiatisée pour SIP dans laquelle les demandes sont envoyées à un serveur dans le domaine local de l'utilisateur, qui authentifie de telles demandes (en utilisant les mêmes pratiques que celles par lesquelles le domaine authentifierait les demandes REGISTER). Une fois qu'un message a été authentifié, le domaine local a alors besoin d'un moyen pour communiquer aux autres entités SIP que l'utilisateur envoyeur a été authentifié et que son utilisation du champ d'en-tête From a été autorisée. Le présent document traite de la façon dont cet imprimatur de l'authentification peut être partagé.

La RFC 3261 décrit déjà une architecture très similaire à cela au paragraphe 26.3.2.2, dans laquelle un agent d'utilisateur s'authentifie à un serveur mandataire local, qui à son tour s'authentifie auprès d'un serveur mandataire distant via un TLS mutuel, créant une chaîne de deux liaisons d'authentification transitive entre le générateur et le domaine distant. Bien que ceci fonctionne bien dans certaines architectures, il y a quelques aspects qui le rendent impraticable. Pour l'un d'eux, la confiance transitive est par nature plus faible qu'une assertion qui peut être validée de bout en bout. Il est possible aux demandes SIP de traverser plusieurs intermédiaires dans des domaines administratifs séparés, et dans ce cas la confiance transitive devient même moins contraignante.

Une solution à ce problème est d'utiliser des intermédiaires SIP de confiance qui affirment une identité pour les utilisateurs sous la forme d'un en-tête SIP privilégié. Un mécanisme pour le faire (avec l'identité P-Asserted-header) est donné dans la [RFC3325]. Cependant, cette solution permet seulement une confiance bond par bond entre les intermédiaires, pas une authentification cryptographique de bout en bout , et elle suppose un réseau géré de nœuds avec des relations de confiance mutuelle stricte, une hypothèse qui est incompatible avec les larges déploiements de l'Internet.

Par conséquent, le présent document spécifie un moyen pour partager une assurance cryptographique de l'identité de l'utilisateur SIP final dans un contexte inter domaines ou intra domaine qui se fonde sur le concept d'un "service d'authentification" et un nouvel en-tête SIP, l'en-tête Identity. Noter que la portée du présent document est limitée à fournir l'assurance d'identité pour les demandes SIP ; résoudre ce problème pour les réponses SIP est plus compliqué et fera l'objet de travaux futurs.

La présente spécification permet à un agent d'utilisateur ou à un serveur mandataire de fournir des services d'identité et de vérifier les identités. Pour maximiser la sécurité de bout en bout, il est évidemment préférable que les utilisateurs acquièrent leurs propres certificats et leurs clés privées correspondantes ; si ils le font, ils peuvent agir comme un service d'authentification. Cependant, les certificats de l'utilisateur final peuvent n'être ni pratiques ni acceptables, étant données les difficultés d'établissement d'une infrastructure de clé publique (PKI, *Public Key Infrastructure*) qui s'étende aux utilisateurs d'extrémité, et de plus, compte tenu du grand nombre potentiel d'agents d'utilisateur SIP (téléphones, ordinateurs personnels, tablettes, ordinateurs portables, consoles de jeux) qui peuvent être employés par un seul utilisateur. Dans ces environnements, la synchronisation du matériel de chiffrement sur plusieurs appareils peut être très complexe et exige beaucoup du comportement du point d'extrémité. Gérer plusieurs certificats pour les divers appareils est aussi assez problématique et impopulaire auprès des utilisateurs. En conséquence, dans l'utilisation initiale de ce mécanisme, il est probable que des intermédiaires vont instancier le rôle de service d'authentification.

4. Vue d'ensemble du fonctionnement

Cette section donne une vue d'ensemble informative (non normative) générale des mécanismes décrits dans le présent document.

Imaginons le cas où Alice, qui a le mandataire de rattachement de exemple.com et l'adresse d'enregistrement de alice@exemple.com, veut communiquer avec sip:bob@exemple.org.

Alice génère un INVITE et place son identité dans le champ d'en-tête From de la demande. Elle envoie ensuite un INVITE sur TLS à un service d'authentification mandataire pour son domaine.

Le service d'authentification authentifie Alice (éventuellement en envoyant une demande d'authentification par résumé) et valide qu'elle est autorisée à affirmer l'identité qu'elle a placée dans le champ d'en-tête From. Cette valeur peut être l'AoR d'Alice, ou ce peut être une autre valeur que la politique du serveur mandataire lui permet d'utiliser. Il calcule ensuite un hachage sur certains en-têtes particuliers, incluant le champ d'en-tête From et les corps du message. Ce hachage est signé avec le certificat pour le domaine (exemple.com, dans le cas d'Alice) et inséré dans un nouveau champ d'en-tête dans le message SIP, l'en-tête "Identity".

Le mandataire, en tant que détenteur de la clé privée de son domaine, affirme que le générateur de cette demande a été authentifié et qu'elle est autorisée à revendiquer l'identité (l'adresse d'enregistrement SIP) qui apparaît dans le champ d'en-tête From. Le mandataire insère aussi un champ d'en-tête d'accompagnement, Identity-Info, qui dit à Bob comment acquérir son certificat, si il ne l'a pas déjà.

Quand le domaine de Bob reçoit la demande, il vérifie la signature fournie dans l'en-tête Identity, et donc peut valider que le domaine indiqué par la portion hôte de l'AoR dans le champ d'en-tête From a authentifié l'utilisateur, et a permis à l'utilisateur d'affirmer cette valeur de champ d'en-tête From. Cette même opération de validation peut être effectuée par le serveur de l'agent d'utilisateur (UAS, *user agent server*) de Bob.

5. Comportement du service d'authentification

Le présent document définit un nouveau rôle pour les entités SIP appelé un service d'authentification. Le rôle de service d'authentification peut être instancié par un serveur mandataire ou un agent d'utilisateur. Toute entité qui instancie le rôle de service d'authentification DOIT posséder la clé privée d'un certificat de domaine. Les intermédiaires qui instancient ce rôle DOIVENT être capables d'authentifier un ou plusieurs utilisateurs SIP qui peuvent s'enregistrer dans ce domaine. Couramment, ce rôle va être instancié par un serveur mandataire, car ces entités vont très probablement avoir un nom d'hôte statique, détenir un certificat correspondant, et avoir accès à des capacités de registraire SIP qui leur permettent d'authentifier les utilisateurs dans leur domaine. Il est aussi possible que le rôle de service d'authentification soit instancié par une entité qui agit comme serveur de redirection, mais cette question est laissée à des travaux futurs.

Les entités SIP qui agissent comme un service d'authentification DOIVENT ajouter un champ d'en-tête Date aux demandes SIP si il n'en est pas déjà présent (voir à la Section 9 des informations sur la façon dont le champ d'en-tête Date aide les vérificateurs). De même, les services d'authentification DOIVENT ajouter un champ d'en-tête Content-Length *(longueur du contenu)* aux demandes SIP si il n'en est pas déjà un présent ; cela peut aider les vérificateurs à faire une double vérification qu'ils hachent exactement autant d'octets de corps de message que le service d'authentification quand ils vérifient le message.

Les entités qui instancient le rôle de service d'authentification effectuent les étapes suivantes, dans l'ordre indiqué, pour générer un en-tête Identity pour une demande SIP :

Étape 1 :
Le service d'authentification DOIT extraire l'identité de l'envoyeur de la demande. Le service d'authentification prend cette valeur dans le champ d'en-tête From ; cette AoR va être appelée ici le "champ d'identité". Si le champ d'identité contient un URI SIP ou SIP sécurisé (SIPS) le service d'authentification DOIT extraire la portion nom d'hôte du champ d'identité et la comparer au domaine pour lequel il est responsable (suivant les procédures du paragraphe 16.4 de la RFC 3261, utilisées par un serveur mandataire pour déterminer le ou les domaines dont il est responsable). Si le champ d'identité utilise le schéma d'URI TEL, la politique du service d'authentification détermine si il est ou non responsable pour cette identité ; voir plus d'informations à la Section 11. Si le service d'authentification n'est pas responsable de l'identité en question, il DEVRAIT traiter et transmettre la demande normalement, mais il NE DOIT PAS ajouter d'en-tête Identity ; voir ci-dessous

plus d'informations sur le traitement pas un service d'authentification d'un en-tête Identity existant.

Étape 2:
Le service d'authentification DOIT déterminer si l'envoyeur de la demande est autorisé ou non à revendiquer l'identité donnée dans le champ d'identité. Pour ce faire, le service d'authentification DOIT authentifier l'envoyeur du message. Les façons possibles d'effectuer cette authentification incluent :

- Si le service d'authentification est instancié par un intermédiaire SIP (serveur mandataire) il peut mettre au défi la demande avec un code de réponse 407 en utilisant le schéma d'authentification Digest (ou envoyant un en-tête Proxy-Authentication envoyé dans la demande, qui a été envoyé en anticipation d'une mise au défi utilisant des accréditifs en antémémoire, comme décrit au paragraphe 22.3 de la RFC 3261). Noter que si ce serveur mandataire entretient une connexion TLS avec le client sur laquelle le client s'est précédemment authentifié en utilisant l'authentification par résumé, la valeur d'identité obtenue de cette étape d'authentification précédente peut être réutilisée sans résumé supplémentaire.
- Si le service d'authentification est instancié par un agent d'utilisateur SIP, un agent d'utilisateur peut être dit authentifier son utilisateur sur la base que l'utilisateur peut provisionner l'agent d'utilisateur avec la clé privée du domaine, ou de préférence en provisionnant un mot de passe qui débloque cette clé privée.

  L'autorisation d'utilisation d'un nom d'utilisateur particulier dans le champ d'en-tête From est une affaire de politique locale pour le service d'authentification, qui dépend largement de la manière dont l'authentification est effectuée. Par exemple, une politique pourrait être comme suit : le nom d'utilisateur donné dans le paramètre "'username"' de l'en-tête Proxy-Authorization DOIT correspondre exactement au nom d'utilisateur dans le champ d'en-tête From du message SIP. Cependant, ceci est dans de nombreux cas trop limitatif ou inapproprié ; un domaine peut utiliser les paramètres "username" dans une Proxy-Authorization qui ne correspond pas à la portion utilisateur des en-têtes SIP From, ou un utilisateur pourrait gérer plusieurs comptes dans le même domaine administratif. Dans ce dernier cas, un domaine pourrait conserver une transposition entre les valeurs dans le paramètre "username" de Proxy-Authorization et un ensemble de un ou plusieurs URI SIP qui pourraient légitimement être affirmés pour cet "username". Par exemple, le nom d'utilisateur peut correspondre à l'identité privée comme définie dans le projet de partenariat de troisième génération (3GPP, *Third Generation Partnership Project*) et dans ce cas le champ d'en-tête From peut contenir l'une quelconque des identités publiques associées à cette identité privée. Dans cette instance, une autre politique pourrait être comme suit : l'URI dans le champ d'en-tête From DOIT correspondre exactement à un des URI transposés associé au "username" donné dans l'en-tête Proxy-Authorization. Diverses exceptions à de telles politiques peuvent apparaître dans des cas comme l'anonymat ; si l'AoR affirmée dans le champ d'en-tête From utilise une forme comme "sip:anonymous@exemple.com", alors le mandataire "exemple.com" devrait authentifier que l'utilisateur est un utilisateur valide dans le domaine et insérer la signature sur le champ d'en-tête From comme d'habitude.

  Noter que cette vérification est effectuée sur addr-spec dans le champ d'en-tête From (par exemple, l'URI de l'envoyeur, comme "sip:alice@atlanta.exemple.com") ; elle ne convertit pas la portion nom d'affichage du champ d'en-tête From (par exemple, "'Alice Atlanta"). Les services d'authentification PEUVENT vérifier et valider aussi le nom d'affichage, et le comparer à une liste de noms d'affichage acceptables qui peuvent être utilisés par l'envoyeur ; si le nom d'affichage ne satisfait pas aux contraintes de la politique, le service d'authentification DOIT retourner un code de réponse 403. La phrase de cause devrait indiquer la nature du problème ; par exemple, "Nom d'affichage inapproprié". Cependant, le nom d'affichage n'est pas toujours présent, et dans de nombreux environnements, les procédures de fonctionnement exigées pour la validation du nom d'affichage peuvent ne pas exister. Pour plus d'informations, voir le paragraphe 13.2.

Étape 3:
Le service d'authentification DEVRAIT s'assurer que tout en-tête Date pré existant dans la demande est précis. La politique locale peut dicter précisément avec quelle précision la date doit être ; une discordance maximum RECOMMANDÉE de dix minutes va assurer que la demande ne va probablement pas tracasser les vérificateurs. Si l'en-tête Date contient une heure différente de plus de dix minutes de l'heure courante notée par le service d'authentification, le service d'authentification DEVRAIT rejeter la demande. Ce comportement n'est pas obligatoire parce que un client d'agent d'utilisateur (UAC) pourrait seulement exploiter l'en-tête Date pour causer l'échec de la vérification d'une demande ; l'en-tête Identity n'est pas destiné à fournir une source de non répudiation ou un enregistrement parfait de quand les messages sont traités. Finalement, le service d'authentification DOIT vérifier que l'en-tête Date tombe dans la période de validité de son certificat. Plus d'informations sur les propriétés de sécurité associées à la valeur de champ d'en-tête Date figurent à la Section 9.

Étape 4:
Le service d'authentification DOIT former la signature d'identité et ajouter un en-tête Identity à la demande, contenant cette signature. Après l'ajout de l'en-tête Identity à la demande, le service d'authentification DOIT aussi ajouter un en-tête Identity-Info. L'en-tête Identity-Info contient un URI à partir duquel son certificat peut être acquis. Les détails sur la génération de ces deux en-têtes sont fournis à la Section 9.

Finalement, le service d'authentification DOIT transmettre le message normalement.

5.1 Identity au sein d'un dialogue et reciblage

Le reciblage est défini en gros comme l'altération de l'URI de demande par les intermédiaires. Plus précisément, le reciblage supplante l'URI cible d'origine par un qui correspond à un utilisateur différent, un utilisateur qui n'est pas autorisé à s'enregistrer sous l'URI cible d'origine. Par cette définition, le reciblage n'inclut pas, par exemple, la traduction de l'URI de demande en une adresse de contact d'un point d'extrémité qui s'est enregistré sous l'URI cible d'origine.

Quand une demande formant un dialogue est reciblée, cela peut causer quelques soucis pour le mécanisme Identity quand il est appliqué aux demandes envoyées dans la direction arrière au sein d'un dialogue. Ce paragraphe expose des considérations non normatives relatives à ce cas.

Quand une demande est reciblée, elle peut atteindre un point d'extrémité SIP dont l'utilisateur n'est pas identifié par l'URI désigné dans la valeur du champ d'en-tête To. La valeur du champ d'en-tête To d'une demande formant dialogue est utilisée comme champ d'en-tête From des demandes envoyées dans l'autre direction durant le dialogue, et est par conséquent l'en-tête qui va être signé par un service d'authentification pour les demandes envoyées dans la direction arrière. Dans les cas de reciblage, si l'URI dans l'en-tête From n'identifie pas l'envoyeur de la demande dans l'autre direction, il va clairement être inapproprié de fournir une signature Identity sur cet en-tête From. Comme spécifié ci-dessus, si le service d'authentification n'est pas responsable du domaine dans le champ d'en-tête From de la demande, il NE DOIT PAS ajouter un en-tête Identity à la demande, et il devrait traiter/transmettre la demande normalement.

Tous les moyens d'anticiper un reciblage, et ainsi de suite, sortent du domaine d'application du présent document, et de même d'avoir une égale applicabilité à la réponse d'identité comme cela se fait pour les demandes dans la direction de retour au sein du dialogue. Par conséquent, aucune directive spéciale n'est donnée ici pour les mises en œuvre concernant le problème de la "partie connectée" ; le comportement du service d'authentification est inchangé si le reciblage s'est produit pour une demande formant dialogue. Finalement, le service d'authentification fournit un en-tête Identity pour les demandes dans le dialogue vers l'arrière quand l'utilisateur est autorisé à affirmer l'identité donnée dans le champ d'en-tête From, et si il ne l'est pas, un en-tête Identity n'est pas fourni.

Pour plus d'informations sur les problèmes de réponse d'identité et l'espace de solutions potentielles, voir [15].

6. Comportement du vérificateur

Le présent document introduit un nouveau rôle logique pour les entités SIP appelées un serveur. Quand un vérificateur reçoit a message SIP contenant un en-tête Identity, il peut inspecter la signature pour vérifier l'identité de l'envoyeur du message. Normalement, le résultat d'une vérification est fourni en entrée d'un processus d'autorisation qui sort du domaine d'application du présent document. Si un en-tête Identity n'est pas présent dans une demande, et si il en est exigé un par la politique locale (par exemple, sur la base d'une politique par domaine d'envoi, ou par utilisateur envoyeur) alors une réponse 428 "Utiliser un en-tête Identity" DOIT être envoyée.

Afin de vérifier l'identité de l'envoyeur d'un message, une entité agissant comme vérificateur DOIT effectuer les étapes suivantes, dans l'ordre spécifié.

Étape 1:
Le vérificateur DOIT acquérir le certificat pour le domaine signant. Les mises en œuvre qui prennent en charge la présente spécification DEVRAIENT avoir un moyen de conserver les certificats de domaine (en accord avec les pratiques normales pour la durée de vie des certificats et leur révocation) afin d'empêcher qu'elles téléchargent inutilement le même certificat chaque fois qu'une demande provenant du même domaine est reçue. Les certificats mis en antémémoire de cette manière devraient être indexés par l'URI donné dans la valeur de champ d'en-tête Identity-Info.

Quand le certificat de domaine utilisé pour signer ce message n'est pas déjà connu du vérificateur, les entités SIP DEVRAIENT découvrir ce certificat en déréférençant l'en-tête Identity-Info, sauf si elles ont un moyen plus efficace spécifique de la mise en œuvre d'acquérir les certificats pour ce domaine. Si le schéma d'URI dans l'en-tête Identity-Info ne peut pas être déréferencé, une réponse 436 "Mauvaises Identity-Info" DOIT être retournée. Le vérificateur traite ce certificat de la façon usuelle, incluant de vérifier qu'il n'est pas expiré, que la chaîne est valide jusqu'à une autorité de certification (CA) de confiance, et qu'il n'apparaît pas sur les listes de révocation. Une fois le certificat acquis, il DOIT être validé suivant les procédures de la [RFC3280]. Si le certificat ne peut pas être validé (si il est auto signé et pas de

confiance, ou signé par une autorité de certification inconnue ou pas de confiance, expiré, ou révoqué) le vérificateur DOIT envoyer une réponse 437 "Certificat non accepté".

Étape 2:
Le vérificateur DOIT suivre le processus décrit au paragraphe 13.4 pour déterminer si le signataire est d'autorité pour l'URI dans le champ d'en-tête From.

Étape 3:
Le vérificateur DOIT vérifier la signature dans le champ d'en-tête Identity, suivant les procédures pour générer le hachage de la chaîne de résumé décrite à la Section 9. Si un vérificateur détermine que la signature sur le message ne correspond pas à la chaîne de résumé reconstruite, une réponse 438 "En-tête Identity invalide" DOIT alors être retournée.

Étape 4:
Le vérificateur DOIT valider les en-têtes Date, Contact, et Call-ID de la manière décrite au paragraphe 13.1 ; les receveurs qui souhaitent vérifier les signatures Identity DOIT prendre en charge toutes les opérations qui y sont décrites. Il doit de plus s'assurer que la valeur de l'en-tête Date tombe dans la période de validité du certificat dont la clé privée correspondante a été utilisée pour signer l'en-tête Identity.

7. Considérations sur l'agent d'utilisateur

Ce mécanisme peut être appliqué de façon opportuniste aux déploiements existants de SIP ; en conséquence, il n'exige aucun changement au comportement de l'agent d'utilisateur SIP pour qu'il soit effectif. Cependant, parce que ce mécanisme ne fournit pas de protection de l'intégrité entre l'UAC et le service d'authentification, un UAC DEVRAIT mettre en œuvre des moyens pour fournir cette protection de l'intégrité. TLS pourrait être un de ces mécanismes, qui est intéressant parce qu'il DOIT être pris en charge par les serveurs mandataires SIP, mais est potentiellement problématique parce qu'il est un mécanisme bond par bond. Voir plus d'informations au paragraphe 13.3 sur la sécurisation du canal entre l'UAC et le service d'authentification.

Quand un UAC envoie une demande, il DOIT remplir précisément le champ d'en-tête From avec une valeur correspondant à une identité dont il croit qu'il est autorisé à la revendiquer. Dans une demande, il DOIT régler la portion URI de son en-tête From à correspondre à une AoR SIP, SIPS, ou TEL qu'il est autorisé à utiliser dans le domaine (incluant des URI anonymes, comme décrit dans la [RFC3323]). En général, les UAC NE DEVRAIENT PAS utiliser la forme d'URI TEL dans le champ d'en-tête From (voir la Section 11).

Noter que le présent document définit un certain nombre de nouveaux codes de réponse 4xx. Si les agents d'utilisateur prennent en charge ces codes de réponse, ils vont être capables de répondre intelligemment aux conditions d'erreur fondées sur Identity.

L'UAC DOIT aussi être capable d'envoyer des demandes, incluant des demandes à mi appel, par un mandataire "externe" (le service d'authentification). La meilleur façon de réaliser cela est d'utiliser des en-têtes Route pré chargées et l'acheminement lâche. Pour un domaine donné, si une entité qui peut instancier le rôle de service d'authentification n'est pas dans le chemin des demandes formant dialogue, l'identité pour les demandes de mi-dialogue dans la direction inverse ne peut pas être fournie.

Comme receveur d'une demande, un agent d'utilisateur qui peut vérifier les identités signées devrait aussi prendre en charge une interface d'utilisateur appropriée pour rendre la validité de l'identité à un utilisateur. Les mises en œuvre d'agent d'utilisateur DEVRAIENT différencier les valeurs de champ d'en-tête From signées des valeurs de champ d'en-tête From non signées quand elles rendent à un utilisateur final l'identité de l'envoyeur d'une demande.

8. Considérations sur les serveurs mandataires

La politique d'un domaine peut exiger des serveurs mandataires qu'ils inspectent et vérifient l'identité fournie dans les demandes SIP. Un serveur mandataire peut souhaiter s'assurer de l'identité de l'envoyeur du message pour empêcher les pourriels ou pour des services de contrôle d'appel. Même si un serveur mandataire n'agit pas comme service d'authentification, il PEUT valider l'en-tête Identity avant de prendre une décision de transmission pour une demande. Les serveurs mandataires NE DOIVENT PAS retirer ou modifier un en-tête Identity ou Identity-Info existant dans une demande.

9. Syntaxe d'en-tête'

Le présent document spécifie deux nouveaux en-têtes SIP : Identity et Identity-Info. Chacun de ces en-têtes peut apparaître seulement une fois dans un message SIP. La grammaire de ces deux en-têtes est (suivant l'ABNF [RFC4234] de la [RFC3261]) :

Identity = "Identity" HCOLON signed-identity-digest
signed-identity-digest = LDQUOT 32LHEX RDQUOT

Identity-Info = "Identity-Info" HCOLON ident-info *(SEMI ident-info-params)
ident-info = LAQUOT absoluteURI RAQUOT
ident-info-params = ident-info-alg / ident-info-extension
ident-info-alg = "alg" EQUAL token
ident-info-extension = generic-param

Le signed-identity-digest *(résumé d'identité signé)* est un hachage signé d'une chaîne canonique générée à partir de certains composants d'une demande SIP. Pour créer le contenu du signed-identity-digest, les éléments suivants d'un message SIP DOIVENT être placés dans une chaîne exacte au bit près dans l'ordre spécifié ici, séparés par une ligne verticale, "|" ou le caractère %x7C :

- L'AoR de l'UA qui envoie le message, ou l'addr-spec du champ d'en-tête From (appelé occasionnellement ici le champ identité).
- Le composant addr-spec *(spécification d'adresse)* du champ d'en-tête To, qui est l'AoR à laquelle la demande est envoyée.
- Le callid *(identifiant d'appel)* provenant du champ d'en-tête Call-Id.
- Les portions digit (1*CHIFFRE) et method (méthode) provenant du champ d'en-tête CSeq, séparées par une seule espace (ABNF SP, ou %x20). Noter que le champ d'en-tête CSeq permet des espaces blanches linéaires (LWS, *linear whitespace*) plutôt que SP pour séparer les portions digit et method, et donc le champ d'en-tête CSeq peut devoir être transformé pour être canonisé. Le service d'authentification DOIT supprimer les zéros en tête de la portion "digit" du Cseq avant de générer la chaîne de résumé.
- Le champ d'en-tête Date, avec exactement une espace pour chaque SP et les éléments de jour et de mois réglés comme montré dans le BNF de la RFC 3261. La RFC 3261 spécifie que le BNF pour les jours de la semaine et les mois est un choix parmi un ensemble de jetons. Les règles de la RFC 2234 pour le BNF spécifient que les jetons sont sensibles à la casse. Cependant, quand ils sont utilisés pour construire la chaîne canonique définie ici, la première lettre de chaque jour et mois DOIT être en majuscule, et les deux lettres restantes doivent être en minuscules. Ceci correspond à la casse fournie dans la définition de chaque jeton. Toutes les demandes qui utilisent le mécanisme Identity DOIVENT contenir un en-tête Date.
- Le composant addr-spec de la valeur de champ d'en-tête Contact. Si la demande ne contient pas d'en-tête Contact, ce champ DOIT être vide (c'est-à-dire, il ne va pas y avoir d'espace entre le quatrième et le cinquième caractère "|" dans la chaîne canonique).
- Le contenu du corps du message avec les bits exactement comme ils sont dans le message (dans l'ABNF pour SIP, le message-body). Cela inclut tous les composants des corps de message multipart. Noter que le message-body N'inclut PAS de CRLF pour séparer les en-têtes SIP du corps de message, mais inclut tout ce qui suit ce CRLF. Si le message n'a pas de corps, le corps de message va être vide, et le "|" final ne va pas être suivi de caractères supplémentaires.

Pour plus d'informations sur les propriétés de sécurité de ces en-têtes, et pourquoi leur inclusion atténue lss attaques en répétition, voir la Section 13 et la [RFC3893]. La formulation précise de cette chaîne de résumé est donc (suivant l'ABNF [RFC4234] de la [RFC3261]) :

digest-string = addr-spec "|" addr-spec "|" callid "|" 1*DIGIT SP Method "|" SIP-date "|" [addr-spec] "|" message-body

Noter que la première addr-spec DOIT être prise dans la valeur du champ d'en-tête From, la seconde addr-spec DOIT être prise de la valeur du champ d'en-tête To, et la troisième addr-spec DOIT être prise de la valeur du champ d'en-tête Contact, pourvu que l'en-tête Contact soit présent dans la demande.

Après que la chaîne de résumé est formée, elle DOIT être hachée et signée avec le certificat pour le domaine. L'algorithme de hachage et de signature est spécifié par le paramètre "alg" de l'en-tête Identity-Info (voir ci-dessous plus d'informations sur les paramètres d'en-tête Identity-Info). Le présent document définit seulement une valeur pour le paramètre "alg" : "rsa-sha1" ; d'autres valeurs DOIVENT être définies dans une RFC sur la voie de la normalisation ; voir plus d'informations au

paragraphe 14.7. Toutes les mises en œuvre de la présente spécification DOIVENT prendre en charge "rsa-sha1". Quand l'algorithme "rsa-sha1" est spécifié dans le paramètre "alg" de Identity-Info, le hachage et la signature DOIVENT être générés comme suit : calculer le résultat de la signature de cette chaîne avec sha1WithRSAEncryption comme décrit dans la [RFC3370] et coder en base64 le résultat comme spécifié dans la [RFC3548]. Une clé RSA de 1024 bits ou plus DOIT être utilisée. Le résultat est placé dans le champ d'en-tête Identity. Des exemples détaillés de l'usage de cet algorithme sont à la Section 10.

La portion "absoluteURI" de l'en-tête Identity-Info DOIT contenir un URI qui déréférence une ressource contenant le certificat du service d'authentification. Toutes les mises en œuvre de la présente spécification DOIVENT prendre en charge l'utilisation des URI HTTP et HTTPS dans l'en-tête Identity-Info. Ces URI HTTP et HTTPS DOIVENT suivre les conventions de la [RFC2585], et pour les URI, la ressource indiquée DOIT être de la forme "application/pkix-cert" décrite dans cette spécification. Noter que cela introduit des problèmes de gestion du cycle de vie des clés ; lorsque un domaine change la clé disponible à l'URI Identity-Info avant qu'un vérificateur évalue une demande signée par un service d'authentification, cela va causer un évident échec du vérificateur. Lorsque un retour à zéro se produit, les services d'authentification DEVRAIENT donc fournir de nouveaux URI Identity-Info pour chaque nouveau certificat, et DEVRAIENT continuer de rendre disponibles les URI d'acquisition des clés plus anciens pendant un temps plus long que la durée de vie plausible d'un message SIP (un heure devrait très probablement suffire).

Le champ d'en-tête Identity-Info DOIT contenir un paramètre "alg". Aucun autre paramètre n'est défini pour l'en-tête Identity-Info dans le présent document. De futures RFC sur la voie de la normalisation pourront définir des paramètres supplémentaires de Identity-Info.

Le présent document ajoute les entrées suivantes au Tableau 2 de la [RFC3261] :

Champ d'en-tête	où	mandataire	ACK	BYE	CAN	INV	OPT	REG	SUB	NOT	REF	INF	UPD	PRA
Identity	R	a	o	o	-	o	o	o	o	o	o	o	o	o
Identity-Info	R	a	o	o	-	o	o	o	o	o	o	o	o	o

Noter que, dans le tableau ci-dessus, ce mécanisme ne protège pas la méthode CANCEL. La méthode CANCEL ne peut pas être mise au défi, parce qu'elle est bond par bond, et en conséquence le comportement du service d'authentification pour CANCEL serait significativement limité. Noter aussi que la méthode REGISTER utilise les champs d'en-tête Contact d'une façon très inhabituelle qui complique son applicabilité à ce mécanisme, et l'utilisation de Identity avec REGISTER est par conséquent un sujet qui sera étudié à l'avenir, bien qu'il soit laissé ici comme facultatif pour des raisons de rétro compatibilité. Les en-têtes Identity et Identity-Info NE DOIVENT PAS apparaître dans CANCEL.

10. Essais et exemples de conformité

Les exemples de cette section illustrent l'utilisation de l'en-tête Identity dans le contexte d'une transaction SIP. Il est conseillé que les mises en œuvre vérifient leur conformité avec la spécification à l'aide des critères suivants :

- La mise en œuvre du rôle de service d'authentification DOIT générer des chaînes d'identité en base64 identiques à celles montrées dans les en-têtes Identity de ces exemples quand elles sont présentées avec le message de source et en utilisant la clé privée appropriée fournie pour le domaine en question.
- Les mises en œuvre du rôle de vérificateur DOIVENT valider correctement les messages donnés contenant l'en-tête Identity quand elles utilisent les certificats fournis (avec l'avertissement sur les certificats auto signés ci-dessous).

Noter que les exemples suivants utilisent des certificats auto signés, plutôt que des certificats produits par une autorité de certification reconnue. L'utilisation de certificats auto signés pour ce mécanisme N'EST PAS RECOMMANDÉE, et elle n'apparaît ici qu'à des fins d'illustration. Donc, dans les essais de conformité, les mises en œuvre de vérificateurs DEVRAIENT générer les avertissements appropriés sur l'utilisation de certificats auto signés. Aussi, les exemples de certificats de cette section ont placé leur nom de domaine sujet dans le champ subjectAltName ; en pratique, les autorités de certification peuvent placer les noms de domaine dans d'autres endroits dans le certificat (voir plus d'informations au paragraphe 13.4).

Noter que tous les exemples de cette section utilisent l'algorithme "rsa-sha1".

Les fichiers de référence au bit près pour ces messages et leurs diverses transformations sont à l'Appendice B.

10.1 Identity-Info avec corps Singlepart MIME

Considérons la paire suivante de clé privée et certificat allouée à "atlanta.exemple.com (rendue en format OpenSSL).

-----DÉBUT DE CLÉ PRIVÉE RSA-----
MIICXQIBAAKBgQDPPMBtHVoPkXV+Z6jq1LsgfTELVWpy2BVUffJMPH06LL0cJSQOaIeVzIojzWtpauB7IylZKlAj
B5f429tRuoUiedCwMLKblWAqZt6eHWpCNZJ7lONcIEwnmh2nAccKk83Lp/VH3tgAS/43DQoX2sndnYh+g8522Pzwg7
EGWspzzwIDAQABAoGBAK0W3tnEFD7AjVQAnJNXDtx59Aa1Vu2JEXe6oi+OrkFysJjbZJwsLmKtrgttPXOU8t2mZpi
0wK4hX4tZhntiwGKkUPC3h9Bjp+GerifP341RMyMO+6fPgjqOzUDw+rPjjMpwD7AkcEcqDgbTrZnWv/QnCSaaF3xkU
GfFkLx5OKcRAkEA7UxnsE8XaT30tP/UUc51gNk2KGKgxQQTHopBcew9yfeCRFhvdL7jpaGatEi5iZwGGQQDVOVH
UN1H0YLpHQjRowJBAN+R2bvA/Nimq464ZgnelEDPqaEAZWaD3kOfhS9+vL7oqES+u5E0J7kXb7ZkiSVUg9XU/8Px
MKx/DAz0dUmOL+UCQH8C9ETUMI2uEbqHbBdVUGNk364CDFcndSxVh+34KqJdjiYSx6VPPv26X9m7S0OydTkSgs
3/4ooPxo8HaMqXm80CQB+rxbB3UlpOohcBwFK9mTrlMB6Cs9ql66KgwnlL9ukEhHHYozGatdXeoBCyhUsogdSU6/aS
AFcvWEGtj7/vyJECQQCCS1lKgEXoNQPqONalvYhyyMZRXFLdD4gbwRPK1uXKYpk3CkfFzOyfjeLcGPxXzq2qzuHz
GTDxZ9PAepwX4RSk
-----FIN DE CLÉ PRIVÉE RSA-----
-----DÉBUT DE CERTIFICAT-----
MIIC3TCCAkagAwIBAgIBADANBgkqhkiG9w0BAQUFADBZMQswCQYDVQQGEwJVUzELMAkGA1UECAwCR0
ExEDAOBgNVBAcMB0F0bGFudGExDTALBgNVBAoMBElFVEYxHDAaBgNVBAMME2F0bGFudGEuZXhhbXBsZ
S5jb20wHhcNMDUxMDI0MDYzNjA2WhcNMDYxMDI0MDYzNjA2WjBZMQswCQYDVQQGEwJVUzELMAkGA1
UECAwCR0ExEDAOBgNVBAcMB0F0bGFudGExDTALBgNVBAoMBElFVEYxHDAaBgNVBAMME2F0bGFudGEu
ZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM88wG0dWg+RdX5nqOrUuyB9MQtVanL
YFVR98kw8fTosvRwlJA5oh5XMiiPNa2lq4HsjKVkqUCMHl/jb21G6hSJ50LAwspuVYCpm3p4dakI1knuU41wgTCeaHa
cBxwqTzcun9Ufe2ABL/jcNChfayd2diH6DznbY/PCDsQZaynPPAgMBAAGjgbQwgbEwHQYDVR0OBBYEFNmU/Mrb
VYcEKDr/20WISrG1j1rNMIGBBgNVHSMEejB4gBTZlPzK21WHBCg6/9tFiEqxtY9azaFdpFswWTELMAkGA1UEBh
MCVVMxCzAJBgNVBAgMAkdBMRAwDgYDVQQHDAdBdGxhbnRhMQ0wCwYDVQQKDARJRVRGMRwwGgYD
VQQDDBNhdGxhbnRhLmV4YW1wbGUuY29tggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgY
EADdQYtswBDmTSTq0mt2117alm/XGFrb2zdbU0vorxRdOZ04qMyrIpXG1LEmnEOgcocyrXRBvq5p6WbZAcEQk0Ds
E3Ve0Nc8x9nmvljW7GsMGFCnCuo4ODTf/1lGdVr9DeCzcj10YUQ3MRemDMXhY2CtDisLWl7SXOORcZAi1oU9w=
-----FIN DE CERTIFICAT-----

Un utilisateur de atlanta.exemple.com, Alice, veut envoyer un INVITE à bob@biloxi.exemple.org. Elle crée donc la demande INVITE suivante, qu'elle transmet au serveur mandataire atlanta.exemple.org qui instancie le rôle de service d'authentification :

```
INVITE sip:bob@biloxi.exemple.org SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.exemple.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.exemple.org>
From: Alice <sip:alice@atlanta.exemple.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.exemple.com>
Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.exemple.com
s=Session SDP
c=IN IP4 pc33.atlanta.exemple.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Quand le service d'authentification reçoit l'INVITE, il authentifie Alice en envoyant une réponse 407. Par suite, Alice ajoute un en-tête Authorization à sa demande, et la renvoie au service d'authentification atlanta.exemple.com. Maintenant que le service est sûr de l'identité d'Alice, il calcule un en-tête Identity pour la demande. La chaîne canonique sur laquelle la signature d'identité va être générée est la suivante (noter que la première ligne est coupée à cause des conventions éditoriales des RFC) :

sip:alice@atlanta.exemple.com|sip:bob@biloxi.exemple.org|
a84b4c76e66710|314159 INVITE|Thu, 21 Feb 2002 13:02:03 GMT|
sip:alice@pc33.atlanta.exemple.com|v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.exemple.com
s=Session SDP
c=IN IP4 pc33.atlanta.exemple.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

La signature résultante (sha1WithRsaEncryption) en utilisant la clé privée RSA donnée ci-dessus, avec le codage base64, est la suivante :

ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2a1pxAr3VgrB0SsSAaifsRdiOPoQZYOy2wrVghuhcs
MbHWUSFxI6p6q5TOQXHMmz6uEo3svJsSH49thyGnFVcnyaZ++yRlBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U=

En conséquence, le service d'authentification atlanta.exemple.com va créer un en-tête Identity contenant cette chaîne de signature base64 (175 octets). Il va aussi ajouter l'URI HTTPS où son certificat est disponible. Avec l'ajout de ces deux en-têtes, le message devient comme suit :

INVITE sip:bob@biloxi.exemple.org SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.exemple.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.exemple.org>
From: Alice <sip:alice@atlanta.exemple.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.exemple.com>
Identity:
"ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2a1pxAr3VgrB0SsSAa
ifsRdiOPoQZYOy2wrVghuhcsMbHWUSFxI6p6q5TOQXHMmz6uEo3svJsSH49thyGn
FVcnyaZ++yRlBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="
Identity-Info: <https://atlanta.exemple.com/atlanta.cer>;alg=rsa-sha1
Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.exemple.com
s=Session SDP
c=IN IP4 pc33.atlanta.exemple.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

atlanta.exemple.com transmet alors la demande normalement. Quand Bob reçoit la demande, si il ne connaît pas déjà le certificat de atlanta.exemple.com, il déréference l'URL dans l'en-tête Identity-Info pour acquérir le certificat. Bob génère ensuite la même chaîne canonique que donné ci-dessus, à partir des mêmes en-têtes de la demande SIP. En utilisant cette chaîne canonique, le résumé signé dans l'en-tête Identity, et le certificat découvert en déréférençant l'en-tête Identity-Info, Bob peut vérifier que l'ensemble d'en-têtes et le corps de message n'ont pas été modifiés.

10.2 Identité pour une demande sans corps ni contact MIME

Considérons la paire suivante de clé privée et certificat allouée à "biloxi.exemple.org".

-----DÉBUT DE CLÉ PRIVÉE RSA-----
MIICXgIBAAKBgQC/obBYLRMPjskrAqWOiGPAUxI3/m2ti7ix4caqCTAuFX5cLegQ7nmquLOHfIhxVIqT2f06UA0lOo
2NVofK9G7MTkVbVNiyAlLYUDEj7XWLDICf3ZHL6Fr/
+CF7wrQ9r4kv7XiJKxodVCCd/DhCT9Gp+VDoe8HymqOW/KsneriyIwIDAQABAoGBAJ7fsFIKXKkjWgj8ksGOthS3S
n19xPSCyEdBxfEm2Pj7/Nzzeli/PcOaic0kJALBcnqN2fHEeIGK/9xUBxTufgQYVJqvyHERs6rXX/iT4Ynm9t1905EiQ9Zp

HsrI/AMMUYA1QrGgAIHvZLVLzq+9KLDEZ+HQbuCLJXF+6bl0Eb5BAkEA636oMANp0Qa3mYWEQ2utmGsYxkX
SfyBb18TCOwCty0ndBR24zyOJF2NbZS98Lz+Ga25hfIGw/JHKnD9bOE88UwJBANBRSpd4bmS+m48R/13tRESAtHqy
dNinX0kS/RhwHr7mkHTU3k/MFxQtx34I3GKzaZxMn0A66KS9v/SHdnF+ePECQQCGe7QshyZ8uitLPtZDclCWhEKHq
AQHmUEZvUF2VHLrbukLLOgHUrHNa24cILv4d3yaCVUetymNcuyTwhKj24wFAkAOz/jx1EplN3hwL+NsllZoWI58u
vu7/Aq2c3czqaVGBbb317sHCYgKk0bAG3kwO3mi93/LXWT1cdiYVpmBcHDBAkEAmpgkFj+xZu5gWASY5ujv+FC
MP0WwaH5hTnXu+tKePJ3d2IJZKxGnl6itKRN7GeRh9PSK0kZSqGFeVrvsJ4Nopg==
-----FIN DE CLÉ PRIVÉE RSA-----
-----DÉBUT DE CERTIFICAT-----
MIIC1jCCAj+gAwIBAgIBADANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTV
MxDzANBgNVBAcMBkJpbG94aTENMAsGA1UECgwESUVURjEbMBkGA1UEAwwSYmlsb3hpLmV4YW1wbGUuY
29tMB4XDTA1MTAyNDA2NDAyNloXDTA2MTAyNDA2NDAyNlowVzELMAkGA1UEBhMCVVMxCzAJBgNVBA
gMAk1TMQ8wDQYDVQQHDAZCaWxveGkxDTALBgNVBAoMBElFVEYxGzAZBgNVBAMMEmJpbG94aS5leGFtc
GxlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAv6GwWC0TD47JKwKljohjwFMSN/5trYu4seHGqg
kwLhV+XC3oEO55qrizh3yIcVSKk9n9OlANJTqNjVaHyvRuzE5FW1TYsgJS2FAxI+11iwyAn92Ry+ha//ghe8K0Pa+JL+
14iSsaHVQgnfw4Qk/RqflQ6HvB8pqjlvyrJ3q4siMCAwEAAaOBsTCBrjAdBgNVHQ4EFgQU0Z+RL47W/APDtc5BfSo
QXuEFE/wwfwYDVR0jBHgwdoAU0Z+RL47W/APDtc5BfSoQXuEFE/yhW6RZMFcxCzAJBgNVBAYTAlVTMQswC
QYDVQQIDAJNUzEPMA0GA1UEBwwGQmlsb3hpMQ0wCwYDVQQKDARJRVRGMRswGQYDVQQDDBJiaWxve
GkuZXhhbXBsZS5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBiyKHIt8TXfGNfpnJX
i5jCizOxmY8Ygln8tyPFaeyq95TGcvTCWzdoBLVpBD+fpRWrX/II5sE6VHbbAPjjVmKbZwzQAtppP2Fauj28t94ZeDH
N2vqzjfnHjCO24kG3Juf2T80ilp9YHcDwxjUFrt86UnlC+yidyaTeusW5Gu7v1g==
-----FIN DE CERTIFICAT-----

Bob (bob@biloxi.exemple.org) veut maintenant envoyer une demande BYE à Alice à la fin du dialogue initié dans l'exemple précédent. Il crée donc la demande BYE suivante, qu'il transmet au serveur mandataire biloxi.exemple.org" qui instancie le rôle de service d'authentification :

BYE sip:alice@pc33.atlanta.exemple.com SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnashds10
Max-Forwards: 70
From: Bob <sip:bob@biloxi.exemple.org>;tag=a6c85cf
To: Alice <sip:alice@atlanta.exemple.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0

Quand le service d'authentification reçoit le BYE, il authentifie Bob en envoyant une réponse 407. Par suite, Bob ajoute un en-tête Authorization à sa demande, et la renvoie au service d'authentification biloxi.exemple.org. Maintenant que le service est sûr de l'identité de Bob, il se prépare à calculer un en-tête Identity pour la demande. Noter que cette demande n'a pas de champ d'en-tête Date. En conséquence, biloxi.exemple.org va ajouter un en-tête Date à la demande avant de calculer la signature d'identité. Si l'en-tête Content-Length n'était pas présent, le service d'authentification l'ajouterait aussi. Le message de base est donc :

BYE sip:alice@pc33.atlanta.exemple.com SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnashds10
Max-Forwards: 70
From: Bob <sip:bob@biloxi.exemple.org>;tag=a6c85cf
To: Alice <sip:alice@atlanta.exemple.com>;tag=1928301774
Date: Thu, 21 Feb 2002 14:19:51 GMT
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0

Noter aussi que cette demande ne contient pas de champ d'en-tête Contact. En conséquence, biloxi.exemple.org ne va pas placer de valeur dans la chaîne canonique pour la spécification d'adresse de l'adresse de Contact. Noter aussi qu'il n'y a pas de corps de message, et en conséquence, la chaîne de signature va se terminer par deux barres verticales. La chaîne canonique sur laquelle va être générée la signature d'identité est la suivante :

sip:bob@biloxi.exemple.org|sip:alice@atlanta.exemple.com|a84b4c76e66710|231 BYE|Thu, 21 Feb 2002 14:19:51 GMT||

La signature résultante (sha1WithRsaEncryption) en utilisant la clé privée RSA donnée ci-dessus pour biloxi.exemple.org, avec codage en base64, est la suivante :

sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dlxkWzoeU7d7OV8HweTTDobV3itTmgPwC
FjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIppPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=

En conséquence, le service d'authentification biloxi.exemple.org va créer un en-tête Identity contenant cette chaîne de signature en base64. Il va aussi ajouter un URL HTTPS où son certificat est disponible. Avec l'ajout de ces deux en-têtes, le message devient maintenant :

BYE sip:alice@pc33.atlanta.exemple.com SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnashds10
Max-Forwards: 70
From: Bob <sip:bob@biloxi.exemple.org>;tag=a6c85cf
To: Alice <sip:alice@atlanta.exemple.com>;tag=1928301774
Date: Thu, 21 Feb 2002 14:19:51 GMT
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Identity:
"sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dlxkWzoeU7d7OV8HweTTDobV3itTmgPw
CFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIppPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs="
Identity-Info: <https://biloxi.exemple.org/biloxi.cer>;alg=rsa-sha1
Content-Length: 0

biloxi.exemple.org transmet alors la demande normalement.

11. Identité et schéma d'URI TEL

Comme de nombreuses applications SIP fournissent un service de voix sur IP (VoIP, *Voice over IP*) les numéros de téléphone sont couramment utilisés comme identité dans les déploiements de SIP. Dans la majorité des cas, ceci ne pose pas de problème pour le mécanisme d'identité décrit dans le présent document. Les numéros de téléphone apparaissent couramment dans la portion de nom d'utilisateur d'un URI SIP (par exemple, "ip:+17005551008@chicago.exemple.com; user=phone"). Ce nom d'utilisateur se conforme à la syntaxe du schéma d'URI TEL ([RFC3966]). Pour cette sorte d'adresse d'enregistrement SIP, chicago.exemple.com est le signataire approprié.

Il est aussi possible qu'un URI TEL apparaisse dans le champ d'en-tête SIP To ou From en dehors du contexte d'un URI SIP ou SIPS (par exemple, "tel:+17005551008"). Dans ce cas, quel signataire est approprié pour l'identité est beaucoup moins clair. Heureusement pour le mécanisme d'identité, cette forme de l'URI TEL est plus courante pour le champ d'en-tête TO et l'URI de demande dans SIP que dans le champ d'en-tête From, car l'UAC n'a pas d'autre option que de fournir un URI TEL seul quand le domaine distant auquel est envoyé une demande est inconnu. Le domaine local, cependant, est généralement connu de l'UAC, et en conséquence, il peut former un champ d'en-tête From approprié contenant un URI SIP avec un nom d'utilisateur de forme URI TEL. Les mises en œuvre qui entendent envoyer leurs demandes par un service d'authentification DEVRAIENT mettre les numéros de téléphone dans le champ d'en-tête From dans des URI SIP ou SIPS chaque fois que possible.

Si le domaine local est inconnu de l'UAC qui formule une demande, il ne sera très probablement pas capable de localiser un service d'authentification pour sa demande, et donc la question de la fourniture de l'identité dans ces cas est un peu discutable. Cependant, un service d'authentification PEUT signer une demande contenant un URI TEL dans le champ d'en-tête From. Ceci est permis dans la présente spécification pour les seuls besoins de compatibilité future. À plus long terme, il est possible que ENUM [RFC3761] puisse fournir un moyen de déterminer quel domaine administratif est responsable d'un numéro de téléphone, et cela peut aider à la signature et vérification des identités SIP qui contiennent des numéros de téléphone. Cela fera l'objet de travaux futurs.

12. Considérations de confidentialité

Le mécanisme d'identité présenté dans le présent document est compatible avec les pratiques standard de SIP pour la confidentialité décrites dans la [RFC3323]. Un serveur mandataire SIP peut agir à la fois comme service de confidentialité et comme service d'authentification. Comme un agent d'utilisateur peut fournir toute valeur de champ d'en-tête From que le service d'authentification veut autoriser, il n'y a pas de raison que des URI SIP privés qui contiennent des domaines

légitimes (par exemple, sip:anonymous@exemple.com) ne puissent pas être signés par un service d'authentification. La construction de l'en-tête Identity est la même pour les URI privés que pour toutes les autres sortes d'URI.

Noter, cependant, qu'un service d'authentification doit posséder un certificat correspondant à la portion hôte de la spécification d'adresse du champ d'en-tête From de toute demande qu'il signe ; en conséquence, utiliser des domaines comme "anonymous.invalid" ne va pas être possible pour les services de confidentialité qui agissent aussi comme service d'authentification. L'assurance offerte par l'usage d'URI anonymes avec une une portion domaine valide est "ceci est un utilisateur connu dans mon domaine, que j'ai authentifié, mais je garde son identité confidentielle". L'utilisation du domaine "anonymous.invalid" entraîne qu'aucune autorité correspondante pour le domaine ne peut exister, et par conséquent, les fonctions de service d'authentification n'ont pas d'objet.

Le niveau de confidentialité "header" décrit dans la RFC 3323 demande qu'un service de confidentialité altère la valeur du champ d'en-tête Contact d'un message SIP. Comme le champ d'en-tête Contact est protégé par la signature dans un en-tête Identity, les services de confidentialité ne peuvent pas être appliqués après les services d'authentification sans qu'il en résulte une violation d'intégrité.

La [RFC3325] définit le jeton de valeur de confidentialité "id", qui est spécifique de P-Asserted-header Identity. La sorte d'assertion fournie par l'identité P-Asserted-header est très différente de l'en-tête Identity présentée dans le présent document. Il contient des informations supplémentaires sur l'envoyeur d'un message qui peuvent aller au delà de ce qui apparaît dans le champ d'en-tête From ; P-Asserted-Identity contient une identité définitive de l'envoyeur qui est en quelque sorte connue d'un réseau clos d'intermédiaires, et le réseau va probablement utiliser cette identité à des fins de facturation ou de sécurité. Le danger que ces informations spécifiques du réseau fuitent hors du réseau clos a motivé le jeton de valeur privée "id". Le jeton de valeur privée "id" n'a pas d'implications sur l'en-tête Identity, et les services de confidentialité NE DOIVENT PAS retirer l'en-tête Identity quand une priv-value de "id" apparaît dans un en-tête Privacy.

On note finalement qu'à la différence de la RFC 3325, le mécanisme décrit dans la présente spécification n'ajoute pas aux demandes SIP d'informations qui aient des implications pour la confidentialité.

13. Considérations sur la sécurité

13.1 Traitement des éléments digest-string

Le présent document décrit un mécanisme qui fournit une signature sur les champs d'en-tête Contact, Date, Call-ID, CSeq, To, et From des demandes SIP. Bien qu'une signature sur le champ d'en-tête From serait suffisante pour sécuriser un URI seul, les en-têtes supplémentaires fournissent la protection contre la répétition et l'intégrité de référence nécessaires pour s'assurer que l'en-tête Identity ne va pas être utilisée dans des attaques de copié-collé. En général, les considérations relatives à la sécurité de ces en-têtes sont les mêmes que celles données dans la RFC 3261 pour inclure les en-têtes dans des corps MIME tunnelés "message/sip" (voir en particulier la Section 23). Les paragraphes qui suivent détaillent les propriétés de sécurité individuelles obtenues en incluant chacun de ces champs d'en-tête dans la signature ; collectivement, cet ensemble de champs d'en-tête fournit les propriétés nécessaires pour empêcher les usurpations d'identité.

Le champ d'en-tête From indique l'identité de l'envoyeur du message, et l'URI de l'adresse d'enregistrement SIP dans le champ d'en-tête From est l'identité d'un utilisateur SIP, pour les besoins du présent document. Le champ d'en-tête TO donne l'identité de l'utilisateur SIP que vise cette demande. Fournir le champ d'en-tête TO dans la signature de Identity a deux objets : d'abord, cela empêche les attaques de copié-collé dans lesquelles un en-tête Identity provenant d'une demande légitime d'un utilisateur est copié-collé dans une demande pour un utilisateur différent ; ensuite, cela préserve le schéma d'URI de début de la demande, ce qui aide à prévenir les attaques en dégradation contre l'utilisation de SIPS.

Les en-têtes Date et Contact fournissent l'intégrité de référence et la protection contre la répétition, comme décrit au paragraphe 23.4.2 de la RFC 3261. Les mises en œuvre de la présente spécification NE DOIVENT PAS réputer valide une demande avec un champ d'en-tête Date périmé (l'intervalle RECOMMANDÉ est que l'en-tête Date doit indiquer une heure dans les 3600 secondes de la réception d'un message). Les mises en œuvre DOIVENT aussi enregistrer les Call-ID reçus dans des demandes valides contenant un en-tête Identity, et DOIVENT se souvenir de ces Call-ID pendant au moins la durée d'un intervalle de Date (c'est-à-dire, normalement 3600 secondes). Parce qu'un UA conforme à SIP ne génère jamais deux fois le même Call-ID, les vérificateurs peuvent utiliser le Call-ID pour reconnaître les attaques de copié-collé ; le Call-ID sert de nom occasionnel. Le résultat de cela est que si un en-tête Identity est répété dans l'intervalle de Date, les vérificateurs vont reconnaître qu'il est invalide à cause d'une duplication de Call-ID ; si un en-tête Identity est répété après l'intervalle de Date, les vérificateurs vont reconnaître qu'il est invalide parce que la date est périmée. Le champ d'en-tête CSeq contient un identifiant numérique de la transaction, et le nom de la méthode de la demande ; sans ces informations,

une demande INVITE pourrait être copiée-collée par un attaquant et transformée en une demande BYE sans changer de champs couverts par l'en-tête Identity, et de plus les demandes au sein d'une certaine transaction pourraient être répétées de façon potentiellement troublante ou malveillante.

Le champ d'en-tête Contact est inclus pour lier l'en-tête Identity à l'instance particulière d'agent d'utilisateur qui a généré la demande. Si un attaquant actif intercepte une demande contenant un en-tête Identity, et copie-colle le champ d'en-tête Identity dans sa propre demande (réutilisant les champs From, To, Contact, Date, et Call-ID qui apparaissent dans le message d'origine) l'attaquant ne serait pas éligible à recevoir des demandes SIP provenant de l'agent d'utilisateur appelé, car ces demandes sont acheminées à l'URI identifié dans le champ d'en-tête Contact. Cependant, l'en-tête Contact n'est inclus que dans les demandes formant dialogue, de sorte qu'il ne fournit pas cette protection dans tous les cas.

Il peut sembler intéressant de fournir une signature sur certaines des informations présentes dans la ou les valeurs de champ d'en-tête Via. Par exemple, sans une signature sur le champ sent-by du champ d'en-tête Via de tête, un attaquant pourrait retirer ce champ d'en-tête Via et insérer le sien dans une attaque de copié-collé, qui serait cause que toutes les réponses à la demande seraient acheminées à un hôte du choix de l'attaquant. Cependant, une signature sur le champ d'en-tête Via de tête n'empêche pas les attaques de cette nature, car l'attaquant pourrait laisser intact le Via de tête et simplement insérer un nouveau champ d'en-tête Via directement après lui, ce qui serait cause que les réponses seraient acheminées à l'hôte de l'attaquant "sur leur chemin" vers l'hôte valide, ce qui a exactement le même résultat final. Bien qu'il soit possible qu'un service d'authentification s'appuyant sur des intermédiaires puisse garantir qu'aucun bond Via n'est inséré entre l'agent d'utilisateur envoyeur et le service d'authentification, il ne pourrait pas empêcher un attaquant d'ajouter un bond Via après le service d'authentification, et par là de préempter les réponses. Il est nécessaire pour le fonctionnement approprié de SIP que les intermédiaires suivants soient capables d'insérer de tels champs d'en-tête Via, et donc cela ne peut pas être empêché. À ce titre, bien que cela soit désirable, sécuriser Via n'est pas possible par la sorte de mécanisme d'identité décrit dans le présent document ; la meilleure pratique connue pour sécuriser Via est d'utiliser SIPS.

Ce mécanisme fournit aussi une signature sur les corps de demandes SIP. La raison la plus importante de faire cela est de protéger les corps du protocole de description de session (SDP) portés dans les demandes SIP. Il y a peu de sens à établir l'identité de l'utilisateur qui a généré une demande SIP si cette assurance n'est pas couplée à une assurance comparable sur les descripteurs de supports. Noter cependant que ce n'est pas une sécurité parfaite de bout en bout. Le service d'authentification lui-même, quand il est instancié sur un intermédiaire, pourrait certainement changer le SDP (et les en-têtes SIP, pour cet objet) avant de fournir une signature. Donc, alors que ce mécanisme réduit les chances qu'un répétant ou interposé modifie SDP, cela ne les élimine pas entièrement. Comme une hypothèse fondatrice de ce mécanisme est que les utilisateurs font confiance à leur domaine local pour assurer leur sécurité, ils doivent aussi faire confiance au service pour ne pas violer l'intégrité de leur message sans de bonnes raisons. Noter que le paragraphe 16.6 de la RFC 3261, déclare que les serveurs mandataires SIP "NE DOIVENT PAS ajouter, modifier, ou supprimer le corps de message".

En dernière analyse, les en-têtes Identity et Identity-Info ne peuvent pas se protéger eux-mêmes. Tout attaquant pourrait retirer ces en-têtes d'une demande SIP, et modifier arbitrairement la demande après coup. Cependant, ce mécanisme n'est pas destiné à protéger les demandes contre un interposé qui interfère avec les messages SIP ; il est destiné seulement à fournir un moyen par lequel les utilisateurs SIP peuvent prouver définitivement qu'ils sont qui ils prétendent être. Au mieux, en supprimant les informations d'identité d'une demande, un interposé pourrait rendre impossible de distinguer un message illégitime qu'il voudrait envoyer des messages envoyés par un utilisateur autorisé. Cependant, cela exige une quantité d'énergie considérablement supérieure pour monter une telle attaque qu'il n'en faut pour monter une usurpation d'identité triviale en copiant juste le champ d'en-tête From de quelqu'un d'autre. Ce mécanisme donne le moyen à un utilisateur autorisé pour fournir l'assurance définitive de son identité, ce qu'un utilisateur non autorisé, un usurpateur, ne peut pas.

Un aspect supplémentaire où l'en-tête Identity-Info ne peut pas se protéger lui-même est le paramètre "alg". Le paramètre "alg" n'est pas inclus dans la chaîne de résumé, et par conséquent, un interposé pourrait tenter de modifier le paramètre "alg". Cependant, il est important de noter qu'empêcher les interpositions n'est pas le but principal de ce mécanisme. De plus, changer le paramètre "alg" pourrait au pire résulter en une sorte d'attaque en dégradation, et au mieux causer la défaillance du vérificateur. Noter qu'un seul paramètre "alg" valide est défini dans le présent document et que donc il n'y a pas actuellement d'algorithme plus faible auquel le mécanisme puisse être soumis. "alg' a été incorporé dans ce mécanisme pour des raisons de compatibilité future au cas où l'algorithme actuel présenterait des faiblesses, et exigerait à l'avenir un remplacement en souplesse.

13.2. Noms et identié d'affichage

En matière de conception d'interface, les agents d'utilisateur SIP peuvent rendre la portion nom d'affichage du champ d'en-tête From d'un appelant comme l'identité de l'appelant ; il y a un précédent significatif chez les interfaces d'utilisateur de

messagerie électronique pour cette pratique. À ce titre, il peut sembler que l'absence d'une signature sur le nom d'affichage est une omission significative.

Cependant, il y a plusieurs cas importants dans lesquels une signature sur le nom d'affichage n'empêche pas l'usurpation d'identité. En premier lieu, un nom d'affichage particulier, comme "Jon Peterson", n'est pas unique au monde ; de nombreux utilisateurs dans différents domaines administratifs peuvent légitimement revendiquer ce nom. De plus, les pratiques de liste d'adhérents pour les services fondés sur SIP pourraient avoir des difficultés à discerner le nom d'affichage légitime pour un utilisateur ; il est sûr de supposer que les usurpateurs vont être capables de créer des comptes SIP avec des noms d'affichage arbitraires. La même situation prévaut dans la messagerie électronique d'aujourd'hui. Noter qu'un usurpateur qui tente de répéter un message avec un en-tête Identity, en changeant seulement le nom d'affichage dans le champ d'en-tête From, serait détecté par les autres mécanismes de protection contre la répétition décrits au paragraphe 13.1.

Bien sûr, un service d'authentification peut appliquer des politiques sur le nom d'affichage même si celui-ci n'est pas signé. La mécanique exacte pour créer et faire fonctionner de telles politiques sort du domaine d'application du présent document. L'effet de cette politique ne serait pas d'empêcher l'usurpation de l'identité d'un identifiant unique particulier comme un URI SIP (car les noms d'affichage ne sont pas des identifiants uniques) mais de permettre à un domaine de gérer les revendications de ses utilisateurs. Si de telles politiques sont mises en application, les utilisateurs ne seraient pas libres de revendiquer un nom d'affichage de leur choix. En l'absence de signature, les attaquants interposés pourraient altérer impunément les noms d'affichage dans une demande. Noter que l'objet de cette spécification est l'attaque d'usurpation d'identité, et cependant, un interposé peut aussi supprimer les en-têtes Identity et Identity-Info d'un message.

Il y a de nombreux environnements dans lesquels des politiques concernant le nom d'affichage ne sont pas faisables. Distribuer des noms d'affichage au bit près et internationalisables aux utilisateurs finaux au titre de leur adhésion ou du processus d'enregistrement exigerait des mécanismes qui ne sont pas explorés dans le présent document. En l'absence de mise en application de politique concernant les noms de domaines, des attaques sont concevables qu'un adversaire pourrait monter contre les systèmes SIP qui s'appuient trop fortement sur le nom d'affichage dans leur interface d'utilisateur, mais cela milite en faveur de la conception d'interface intelligente, et non de changer le mécanisme. S'appuyer sur un identifiant non unique pour l'identité résulterait en fin de compte en un mécanisme faible.

13.3 Sécurisation de la connexion au service d'authentification

L'assurance fournie par ce mécanisme est plus forte quand un agent d'utilisateur forme une connexion directe, de préférence sécurisée par TLS, avec un service d'authentification s'appuyant sur des intermédiaires. La raison en est double :

- Si un utilisateur ne reçoit pas de certificat du service d'authentification sur cette connexion TLS qui corresponde au domaine attendu (en particulier quand l'utilisateur reçoit un défi via un mécanisme comme Digest), il est alors possible qu'un serveur félon tente de se faire passer pour un service d'authentification pour un domaine qu'il ne contrôle pas, tentant éventuellement de collecter des secrets partagés pour ce domaine.
- Sans TLS, les diverses valeurs de champ d'en-tête et le corps de la demande n'auront pas de protection de l'intégrité quand la demande arrivera à un service d'authentification. En conséquence, un intermédiaire antérieur légitime ou illégitime pourrait modifier arbitrairement le message.

De ces deux problèmes, le premier est le plus réel pour la portée prévue de ce mécanisme. Ce mécanisme est destiné à empêcher les attaques d'usurpation d'identité, pas les attaques par interposition ; l'intégrité sur l'en-tête et les corps est fournie par ce mécanisme pour empêcher seulement les attaques en répétition. Cependant, il est possible que les applications qui s'appuient sur la présence de l'en-tête Identity puissent développer cette protection de l'intégrité, en particulier l'intégrité du corps, pour des services autres que la protection contre la répétition.

En conséquence, des connexions TLS directes DEVRAIENT être utilisées entre l'UAC et le service d'authentification chaque fois que possible. La nature opportuniste de ce mécanisme, rend cependant très difficile de contraindre le comportement de l'UAC, et de plus, il va y avoir des architectures de déploiement où la connexion directe est simplement infaisable et où l'UAC ne peut pas agir lui-même comme un service d'authentification. En conséquence, quand une connexion directe et TLS ne sont pas possibles, un UAC devrait utiliser le mécanisme SIPS, le résumé "auth-in"' pour l'intégrité du corps, ou les deux quand il peut. La décision ultime d'ajouter un en-tête Identity à une demande appartient bien sûr au service d'authentification ; la politique du domaine doit identifier les cas où l'association de sécurité de l'UAC avec le service d'authentification est trop faible.

13.4 Noms de domaines et subordination

Quand un vérificateur traite une demande contenant un en-tête Identity-Info, il doit comparer la portion domaine de l'URI

dans le champ d'en-tête From de la demande avec le nom de domaine qui est le sujet du certificat acquis de l'en-tête Identity-Info. Bien qu'il semble que ce devrait être un processus direct, il est compliqué par deux réalités de déploiement. En premier lieu, les certificats ont diverses façons de décrire leur sujet, et ils peuvent bien sûr avoir plusieurs sujets, en particulier dans le cas d'un "hébergement virtuel" où plusieurs domaines sont gérés par une seule application. En second lieu, certains services SIP peuvent déléguer les fonctions SIP à un domaine subordonné et utiliser les procédures de la [RFC3263] qui permettent à des demandes pour, par exemple, "exemple.com" d'être acheminées à "sip.exemple.com". Par suite, un utilisateur avec l'AoR "sip:jon@exemple.com" peut faire traiter ses demandes par un hôte comme "sip.exemple.com", et il se peut que ce dernier hôte agisse comme service d'authentification.

Pour traiter le second de ces problèmes, un domaine qui déploie un service d'authentification sur un hôte subordonné DOIT accepter de fournir à cet hôte le matériel de clé privée associé à un certificat dont le sujet est un nom de domaine qui corresponde à la portion domaine des AoR que le domaine distribue aux utilisateurs. Noter que cela correspond au cas comparable de demandes SIP d'acheminement entrant dans un domaine. Quand les procédure de NAPTR et de SRV de la RFC 3263 sont utilisées pour diriger les demandes sur un nom de domaine autre que le domaine qui est dans l'URI de demande d'origine (par exemple, pour "sip:jon@exemple.com", les enregistrement SRV correspondants pointent sur le service "sip1.exemple.org") le client s'attend à ce que le certificat repassé dans tout échange TLS avec cet hôte corresponde exactement au domaine de l'URI de demande d'origine, et non au nom de domaine de l'hôte. Par conséquent, afin de faire fonctionner l'acheminement entrant pour de tels services SIP, un administrateur de domaine doit de même accepter de partager la clé privée du domaine avec le service. Cette décision de conception a été prise pour compenser l'insécurité du DNS, et elle rend certaines approches potentielles de l'hébergement virtuel fondé sur le DNS non sûres pour SIP dans des environnements où les administrateurs de domaine ne veulent pas partager les clés avec les services d'hébergement.

Un vérificateur DOIT évaluer la correspondance entre l'identité de l'utilisateur et le certificat qui signe en suivant les procédures définies au paragraphe 3.1 de la [RFC2818]. Bien que la RFC 2818 traite de l'utilisation de HTTP dans TLS, les procédures décrites sont applicables à la vérification de l'identité si on substitue un en-tête Identity au "nom d'hôte du serveur" dans HTTP pour la portion domaine de l'identité de l'utilisateur dans le champ d'en-tête From d'une demande SIP.

Parce que les certificats de domaine qui peuvent être utilisés par les services d'authentification ont besoin d'affirmer seulement le nom d'hôte du service d'authentification, les autorités de certification existantes peuvent fournir des certificats adéquats pour ce mécanisme. Cependant, tous les serveurs mandataires et agents d'utilisateur ne vont pas être capables de prendre en charge les certificats racines de toutes les autorités de certification, et de plus il y a des différences significatives dans les politiques par lesquelles les autorités de certification produisent leurs certificats. Le présent document ne fait pas de recommandation pour l'usage d'autorités de certification particulières, ni ne décrit de politique particulière que devraient suivre les autorités de certification, mais il est prévu que l'expérience du fonctionnement va créer des standard de fait pour les services d'authentification. Certaines fédérations de fournisseurs de services, par exemple, pourraient ne faire confiance qu'aux certificats qui ont été fournis par une autorité de certification gérée par la fédération. Il est fortement RECOMMANDÉ que les certificats de domaine auto signés ne devraient pas être crus par les vérificateurs, sauf si un échange de clé antérieur a justifié cette confiance.

Pour plus d'information sur la sécurité et les pratiques de certificat, voir la [RFC3280]. Les considérations sur la sécurité de la RFC 3280 sont applicables au présent document.

13.5 Stratégies d'autorisation et de transition

En fin de compte, la valeur de l'assurance fournie par un en-tête Identity est limitée par les pratiques de sécurité du domaine qui produit cette assurance. S'appuyer sur un en-tête Identity généré par un domaine administratif distant suppose que le domaine producteur a utilisé ses pratiques administratives pour authentifier ses utilisateurs. Cependant, il est possible que certains domaines mettent en œuvre des politiques qui en fait rendent les utilisateurs incontrôlables (par exemple, celles qui acceptent des enregistrements non authentifiés provenant d'utilisateurs arbitraires). La valeur d'un en-tête Identity provenant de tels domaines est douteuse. Bien qu'il n'y ait pas de moyen magique pour qu'un vérificateur distingue le "bon" domaine du "mauvais" en inspectant une demande SIP, il est prévu que de futurs travaux sur les pratiques d'autorisation pourraient être construits par dessus cette solution d'identité ; sans une telle solution d'identité, de nombreuses approches prometteuses de la politique d'autorisation sont impossibles. Ceci dit, il est RECOMMANDÉ que les services d'authentification fondés sur les serveurs mandataires emploient de fortes pratiques d'authentification comme les identifiants fondés sur le jeton.

On ne peut pas s'attendre à ce que les en-têtes Identity et Identity-Info soient pris en charge par toutes les entités SIP du jour au lendemain. Cela met le vérificateur dans une position compromettante ; quand il reçoit une demande provenant d'un utilisateur SIP, comment peut il savoir si le domaine de l'envoyeur prend en charge ou non Identity ? En l''absence d'une prise en charge généralisée de Identity, des stratégies de transition sont nécessaires.

Un vérificateur pourrait se souvenir de quand il reçoit une demande provenant d'un domaine qui utilise Identity, et à l'avenir, voir les messages reçus de ce domaine sans en-tête Identity avec scepticisme.

Un vérificateur pourrait interroger le domaine par une sorte de système de rappel pour déterminer si il fait ou non fonctionner un service d'authentification. Il y a un certain nombre de façons potentielles dont ceci pourrait être mis en œuvre ; l'utilisation de la méthode SIP OPTIONS est une possibilité. Ceci fera l'objet de travaux futurs.

À long terme, une sorte de mécanisme d'identité, soit celui documenté dans la présente spécification, soit un successeur, doit devenir d'utilisation obligatoire pour le protocole SIP ; c'est le seul moyen de garantir que cette protection peut toujours être attendue par les vérificateurs.

Finalement, on notera que la présence ou l'absence des en-têtes Identity ne peut pas être le seul facteur de la décision d'autorisation. Des permissions pourraient être accordées à un message sur la base de l'identité spécifique vérifiée ou sur tout autre aspect d'une demande SIP. Les politiques d'autorisation sortent du domaine d'application de la présente spécification, mais cette spécification conseille que le futur travail sur l'autorisation ne suppose pas que les messages avec des en-têtes Identity valides sont toujours bons.

14. Considérations relatives à l'IANA

Le présent document demande des changements aux sous registres d'en-tête et de code de réponse des paramètres SIP du registre de l'IANA, et demande la création de deux nouveaux registres pour les paramètres de l'en-tête Identity-Info.

14.1 Noms de champ d'en-tête

Le présent document spécifie deux nouveaux en-têtes SIP : Identity et Identity-Info. Leur syntaxe est donnée en Section 9. Ces en-têtes sont définis par les informations suivantes, qui ont été ajoutées au sous registre d'en-têtes à http://www.iana.org/assignments/sip-parameters .

Nom d'en-tête : Identity
Forme compacte : y
Nom d'en-tête : Identity-Info
Forme compacte : n

14.2 Code de réponse 428 "Utiliser l'en-tête Identity"

Le présent document enregistre un nouveau code de réponse SIP, qui est décrit en Section 6. Il est envoyé quand un vérificateur reçoit une demande SIP n'a pas d'en-tête Identity afin d'indiquer que la demande devrait être renvoyée avec un en-tête Identity. Ce code de réponse est défini par les informations suivantes, qui ont été ajoutées au sous registre de méthode et code de réponse sous http://www.iana.org/assignments/sip-parameters .

Numéro de code de réponse : 428
Phrase de cause par défaut : Utiliser l'en-tête Identity

14.3 Code de réponse 436 "Mauvaises Identity-Info"

Le présent document enregistre un nouveau code de réponse SIP, qui est décrit en Section 6. Il est utilisé quand l'en-tête Identity-Info contient un URI qui ne peut pas être déréférencé par le vérificateur (soit le schéma d'URI n'est pas pris en charge par le vérificateur, soit la ressource désignée par l'URI est par ailleurs indisponible). Ce code de réponse est défini par les informations suivantes, qui ont été ajoutées au sous registre des méthodes et codes de réponse à http://www.iana.org/assignments/sip-parameters .

Numéro de code de réponse : 436
Phrase de cause par défaut : Mauvaises Identity-Info

14.4 Code de réponse 437 "Certificat non pris en charge"

Le présent document enregistre un nouveau code de réponse SIP, qui est décrit en Section 6. Il est utilisé quand le vérificateur ne peut pas valider le certificat référencé par l'URI de l'en-tête Identity-Info, parce que, par exemple, le certificat est auto-signé, ou signé par une autorité racine de certification pour laquelle le vérificateur ne possède pas de certificat de racine. Ce code de réponse est défini par les informations suivantes, qui ont été ajoutées au sous registre des méthodes et codes de réponse à http://www.iana.org/assignments/sip-parameters .

Numéro de code de réponse : 437
Phrase de cause par défaut : Certificat non pris en charge

14.5 Code de réponse 438 "En-tête Identity invalide"

Le présent document enregistre un nouveau code de réponse SIP, qui est décrit en Section 6. Il est utilisé quand le vérificateur reçoit un message avec une signature Identity qui ne correspond pas à la chaîne de résumé calculée par le vérificateur. Ce code de réponse est défini par les informations suivantes, qui ont été ajoutées au sous registre des méthodes et codes de réponse à http://www.iana.org/assignments/sip-parameters .

Numéro de code de réponse : 438
Phrase de cause par défaut : En-tête Identity invalide

14.6 Paramètres Identity-Info

L'IANA a créé un nouveau registre pour les en-têtes Identity-Info. Ce registre est pré rempli avec une seule entrée pour un paramètre appelé "alg", qui décrit l'algorithme utilisé pour créer la signature qui apparaît dans l'en-tête Identity. Les entrées du registre doivent contenir le nom du paramètre et la spécification dans laquelle le paramètre est défini. Les nouveaux paramètres pour l'en-tête Identity-Info peuvent seulement être définis par des RFC sur la voie de la normalisation.

14.7 Valeurs de paramètre d'algorithme Identity-Info

L'IANA a créé un nouveau registre pour les valeurs du paramètre Identity-Info "alg". Ce registre est pré rempli avec une seule entrée pour une valeur appelée "rsa-sha1", qui décrit l'algorithme utilisé pour créer la signature qui apparaît dans l'en-tête Identity. Les entrées du registre doivent contenir le nom de la valeur du paramètre "alg" et la spécification dans laquelle la valeur est décrite. De nouvelles valeurs pour le paramètre "alg" peuvent seulement être définies par des RFC sur la voie de la normalisation.

Appendice A. Remerciements

Les auteurs tiennent à remercier Eric Rescorla, Rohan Mahy, Robert Sparks, Jonathan Rosenberg, Mark Watson, Henry Sinnreich, Alan Johnston, Patrik Faltstrom, Paul Kyzviat, Adam Roach, John Elwell, Aki Niemi, et Jim Schaad de leurs commentaires. Jonathan Rosenberg a fourni des corrections détaillées à d'innombrables paragraphes du document. L'archive présentée dans l'Appendice B suit l'exemple d'avant garde de la [RFC4475]. Merci à Hans Persson et Tao Wan de leur relecture serrée.

Appendice B. Archive au bit près des exemples de messages

Le bloc de texte suivant est une archive TAR codée, compressée avec gzip, des fichiers qui représentent les transformations effectuées sur les exemples de messages discutés à la Section 10. Il inclut pour chaque exemple :

- (foo).message : le message d'origine
- (foo).canonical : la chaîne canonique construite à partir de ce message
- (foo).sha1 : le hachage SHA1 de la chaîne canonique (en hexadécimal)
- (foo).signed : le hachage signé par RSA de la chaîne canonique (en binaire)
- (foo).signed.enc : le codage en base64 du hachage SHA1 signé par RSA de la chaîne canonique comme elle apparaîtrait dans la demande
- (foo).identity : le message original avec l'ajout des en-têtes Identity et Identity-Info

Deux paires de clé publique/certificat sont aussi incluses dans l'archive, respectivement, pour atlanta.exemple.com et biloxi.exemple.org, incluant :
o (foo).cer : le certificat du domaine
o (foo).privkey : la clé privée du domaine
o (foo).pubkey : la clé publique du domaine, extraite du fichier cert par convention.

Pour récupérer intact le fichier d'archive compressé, le texte du présent document peut être passé en entrée au script Perl suivant (le résultat devrait être redirigé sur un fichier ou entré sur "tar -xzvf -").

```
 #!/usr/bin/perl
use strict;
my $bdata = "";
use MIME::Base64;
while(<>) {
 if (/-- DÉBUT D'ARCHIVE DE MESSAGE --/ .. /-- FIN DE L'ARCHIVE DE MESSAGE --/) {
    if ( m/^\s*[^\s]+\s*$/) {
       $bdata = $bdata . $_;
    }
  }
}
print decode_base64($bdata);
```

Autrement, le bloc codé en base-64 peut être édité manuellement pour retirer les lignes de structure du document et l'entrer dans tout utilitaire de décodage de base-64.

B.1 Fichiers de référence codés

-- DÉBUT D'ARCHIVE DE MESSAGE --
H4sICFfaz0QCA25ld2lkZW50LnRhcgDsW0us5NhZ7gUSwqiF2CAhFikiIQhFt992+U46it+u8qPK5Uc9WPlVfj/KdpXtom
EDCxaAhFggISE2WSHCIoIFioQQC8gqAhRAQQTY8JJAbMgGIYTv7b7T09PT0xNl+mqS3F8qVd3jY/uc85//+87/nXOL
oIv9oGjBB2/PIAiDSBwfv1GERInxG8EwAh6/37UHMIQRKIljCI4+gGCUGKtP8Ad3YKemderJ5EFSBW1QN2Xxmnp5
GtblqXqUPfIffBdZcet/p82conUee0H9sfsfhiACw17nfwQay+Dra+MkQGFkrI+TOPJgAt37/63bo2tjeHGuTVh+bc6FOUub/
E0poM7nLGqyLJ06Id3NGTocPxytMWF6jNJYpDqIoXVLoDlmr+pNx+o7ztZ1ke8WtnXhFUClU5GGLZ6lO3YN8T3P0
Usm1GyG9lQGEiBXFE6+yPecSSvPykuV4TPB5ne9xNEO8KxQVXnk3cqn/TaK3C3T7A08cRGokyJPUzmrV7k5pHK7i
5bQyOambNcDLxUmH9zMD2sl8FGa+WGtBG6bGe5nHafvFnK5n0dnT6N1nmF0mgt3EK3OxQVdiuMzZrNOhPxNOF3
7W7w4LmsLOA0Mpeqt7RTKTrDX1CztZgezbM7rLlvQeBnhWzWOV5qDZEdMahLZTo8Wq0oZOL4XFgkgMhY4pNB
dU53sHVvlaIX5TjqH0+JkYXAXmmzgSI7H9N3RvHingrIOAUIzCph4GhsdHGDwET+WCO5SuDtwxXKNvneGYrWiQ
5WhaTEJXb0LXb6Trgd2DS0ZZscLWm6Bau3aO48HZK4GEWgzN2oRTuBaG/vLXA+aZKh8kDBYyJj7bHWREXgjM
WxIgFQrxPyxb3eUc3EEH6iEptuYL1zFRCpr22rPXujFs9EPx0s+o67pbhzRa/eOjvEZX+wjt1hHgKpDHdvdXJA5er1Y22t
RXXed+KwyxzFadFtZyW1st4E7V7ROO4Rqw5Cnx6ncXb/Z5ztdUOmx34dX3Ck8cydPc76+a5uO4XLTMI9Q3iIwDJBO
loNbUahd5OK7FnQu637tL/cQdlSHel5tRVjh84Jfhl7pDfV2zZyPeEVs3D3t8XoKAVzDo3YAad6sp4r8nCUbUmxUUWA
L9lRiS848gHAm+nZNcQF78RIY2lk6qq6DnFO30Q4B2JaLG2WTkcZ2uVx7ezqGS4vqngA30c5r3KsI8ODevsvtFf6v6vic
BsMd8j+ME+Qt/0PjAnCsT5AQes//d8z/a4OerNZze4z+iczvXqwBtvrI+7TMhDq3WqlMK9nlKt3a0z2RHGGlCQ8jMtubak
AY2zocFupKgghFgbyFoS8BZx7Yl3mZXDZt5ZwYcj5kezmjEwY/YCO4rk+lFQc+26mK7GYb+rhviUDaVKy2X5DZUv
OAOd8VeYQUtOfJ6QxVKtCW0DakDRBDOb3cIk3hF7toGs5wBFldupDkxU1TXS7dnKN1mgFumFWGNmhb8AJH0o
mt08VC23Jtj1O0A9snZMFvA6KMp8s6FYZmkbj7RdcoudzWYdsCq+3SmrVIvq9iqJOxaIu1+6ho406UU2vFohHFJNVU
DOr4sEIxeK0O6nJKHFZhclxeLK4DpvUqSdSqG1+eerx35ELXrPfF5gzqBWs4joD2qSUehFTp8aXsremUp0mrLxp+tnV
MFALaFWhZHg6HWorIohz2um5KZcV4QUcNh4BdC9HZV8ikckSn5WM83neiONKavbQlS4MlANoplaQn67JbMLQ2X
SPumQa1OD9iBLYPiyDjudXR4en9xuHQdHmIDGp6VsjyyBvTE85DwIJMty65T2PDtkJqa4GzVa/KPcjRF8i38qUytVhd
mrEUb1rqHDnx7lFyGd+2RC1FCYwFOMErfKO3oymKyceFn8Q7oyfs1eqMEFsqJw1oOfhmaoQNCmJluerLmeSox20+g
1idmdZA7zKolVXLMvKYTpCp3KwzlSHYhjpmBCGHXZEp1CnlI0nalZdxHPxtUDLsEFlNGfqGBRCgY9CCd97wYpu
Q4HlY8Kyus6wBZ3LIb0tNXx2XmpOdd9EwqPv1VlB8Dgvdbr2S4dNWBnZVirLpQbgsh0MSKJ646reXI3K8nKSLaHL9
nlrRQdVtsbWRviDVDwyrTzD+n9yPGf7fhP8j5kO3+I/AN/k/gZHYPf7fMf6vLEaZs+
+FfvGg0pDIGkfRmLsj2PLX6R5NY6JGcywT6x9OCcDrOOGjUgLwOk74qJQAvJYT3o3O93f6e3b958ZZ2cdvQ/55s/6D
vEf/QbBr/YeAifv4/yToP3DCsnQyfZP+s32j/mOO6Tp3ub75uf6TLipXpDDH5DWVbp7VCzvesGxrnfDuWEEErgvprjN2e
da4aFS9PzVXGWzLmTSsmvSgcTQyfgYtK6/LkOsy4D2FnX15k4AAm6p+k9Y/FxD2LOBs+nMgph+o/YgXev+u9pM/74
6BZ4EotJ7YZ0qunQHXZJni8v5B4wWaXjKJTnfhLmWvRYMzIXYbFjI5jFzInZwlZZR0gmoAGoi39e6ENYEkHsO0UyJ
7umXRkl/i+LGOLxE6zD3bkFOqoJYZrS3Mo5bYjjSc16cLjwvABjZ3TbgwEIHu51MYjruBLihkPUwjBwTDKJjJ0MqZLp
QpjMVG40i2HhaHDtNTcH08ZDpASGdmVh2T7DzUC/SINbE6epSnaWfJNGP36oT2b+QcHeOFULeg/XStYOQGpFdc6
+EMcDBKfXviBR7sukN3IxIljBR2fkm/UvlF3SHaEOu9Kng98MJNO5POObPM9s20E9IU2zrbVNVXduLbrRP35fLmVfY

CXdZ9mrHGr+yzi5y5+n7CIsCNRdBx901oTYGirG/vMgJcPmP/XeqHOxIMszduZuT2I2qEqFtsYT9j4suzz3WwHhFkxa4
eV4ATDkcJN0Tub7Obil4xiVww3PVTrTb0F53O84Qlbcl16TBnsXHb33UWn26oCVojgnBJk1lLYPuAkDTkfL8mhkBJ2i
WCpiC5OB8ScQXFWUTvJ47o+sYS6nRFWkbHTIfaBwTGDU7PBxRN5hsMn97rPvb3K/29B/nmz/kOit/wPI+NaYFz/49j
9/s8nR/8Jb/UfFixdZqes1VXSpDV93CxjcUVb/RwFc6SNybjHPOfImvRJ2OKeEoQ6QBb58aQspcM86u350UQOEGHRU
LYsEc0uDzIlkqqZ2q6txQOdKTuL4xNyu1G4OXtA95ICEEINTlmB7GqdqrH0TG7jhdyXvs2yPshFrEmJ1dTmymAmDflx
uQHlpgjqeJi/pP8syEMjzOWtnCabMJmljbhsIwM1CpjqVwY78D7TH/gcWSUkqF0uQRaDK2/pxB6UAouR+r3iqCEHiQ/
mogxSvcX05ukQ6jt7cTwPEr9uiHq7BWMT2xU51cIUhPOxTu0rqannADguEKwdDeu1GNJz6bxXbOVynFKywvH7qaS7
J1ZZbIUp4WYQ7+LMtf5DoESp0loF6Q4K5LsNryOnNhebXZ9ujcPAuPDMZJcd2w5Q4TNrBLsMy4WAaO7eoGbKZSo
6CB4d5mIHLiQZKDjKXfKzmXWj/zBro/IxNzemOTZbgzDarnmDbqXj4GtxsYVSA1xHnVSTeSqZFpqCKiD0etuj2BwV
5Yuz79UCoglCNqgzaEh+IUyD1Y2YIgak3kTDfnaKW2XV7jkvYzcRL0vAkdal3OL3Z0tAbEmp3VOqKMtQsmpJcxDM
mytnzEcHh7WtoB1yzTsNZhfJCYJ1Ap3SS+ACJj3MV5mGRp0y1Zos25ebOT47nU8kSB8RD/UuR8cWGddFYbKR2F0o
p5BLi2jaLdE8BigUVLYbE/b8eGdXOeNJ3M1I51WYCsm035/wcEMbO/yUnKcCq66gTedIeGQW29O0lQNgtUB9ZL7Y
y71YZETcymuNFIN1RK0MGUr3Y5osBHZ9bhaYVlYvEewnVwN6Bf8/fvnnW9N/yBv9B8Wge/z/jtB/Xk8JwOs44aNSA
vA6TviolAC8lhPu9Z9X4n8IHntOURax52R3G//jAvD5+S8MxbGb9R8K38f/nVgTV1du6X7+OfwHvZNXWfC4rMOn15e
cLPaCz9/uDdxe9cr8qTPDXMwjiYAgRtx+iqDwhNnxT83o9DMTBJ4IgTtBRkdPYOwKpq5weCKq5tOn9wnXJzn+b37F7
cdM/2/M/2AUe3H+E7vZ/0eg+/2fO7ExZicvAr3yUPTxB0T7xJivQOQx9BCwY+fq9i/QVIwJTI2/HiOPsXfc2im86MmFik
TMlQunifwGHm9Rnf6RUNadU/vN1YQcS4S6zK8mTOlOPvt6/PncO60TPnEIb4Z7h4eAWV5N6OtGPrvntcD07LaxVTM
UgkkSewhwThtcTT4UmB4CrJNlj+bc1eRlXBsvGMHxavIc3h4C8+chcjX5dHPGWbOEcPlYGXkrtajv8fEShNmNaezbQk
RjewoX+alWtjYo5e2gGaTS1iHlZ326uZQPgckLCyzSJ5f2TOoC0+RK10bj1szDVccKicPn6sDPUZ80Bg2BB40rEX4NLs
9h20HKCfeaefXSw6rVcRnCp23hXyRXJPM1sc4oprAi6XSw126Fw2qBdlB4sJonn37Rp0fz4jCO8mejtq2aKxB81Sfv2SX
63DtOFj6pG+dREznwOE5l0Y6PeaQERdhGV5Nx6O7R9TsM//OgaZwwuOP9Pwh7cf57hH7i5vw3gd/j/z3+fyz4/1Gh/XsS
wV6K/2skfwvveFP8QyRxm/9hY43r+Efg+/Ofd2KGRMM/9VLu/5knkwM5IyjUP6A4jPuI5wfU
GEw4jsEocX2ghnQdGMbgA3bP8N9l8R+HReDfefwj7/7/H0ZCOPHs/A95H/93YV/6P0b7Veqnf3f9W3/5n9/42+/75f/65g/
4f3X4+p/9w0/8wt8Mv/97f/jX/zt88Stf+/Ljv/unb379+OvZvw3aN/7jn59+6vt/Q7n6sU3/RS36oT/5cS+a/8pXGLL7gy+ReY1
dET/8qa/
+8Q9Wf/HlP6r/9DNf+J9f+8Wf/c3f/vs/z4p/Eb8Q/PePfu2Xfu53rB/59381fvIfH05+Xr6PwE9c/D8OCu9u4/+F/nt9BOBG/y
Xuz//djf77bYoYwLcrXADfilhxv+B4a/EfF+e4fTtbQG+Kfxy6Pv+D4SiMosTN+V9yzAnu4/9O4v9DN3k+ZHfoffs/6JgQ4
NRkrtlz84N2gdArCLmC0JtdoDfrDU/PT8bsu3xiNUFN/3875/PaNBiH8Yt6CBS0Q2SDYcYEkSl9k75Nmkmn7ebWde2W
Lm3646Jp2q7FtU2btq496EGcKMgu4sH5a4dN8NccCMLYP6AMwcv+Bg/e1NMuZimTdlvXyWxx4/s5pQ0N5SXPk/d9nr
claSuHrBhbaKb6cHiUHOYxWe8SBkK1CTFVTWbSpDDAGwjZ1vATeRvaWPWnbFIhmsyQmKNYmhz38Sa7yG+ckG
y5vJKSlF5E8v0ev8mq3bwHPCTYqv9mVEAN9//p+Z+mf9qCMMvqv/
+k4fnfEiqCJbcJfVPnuyR/9XS0YxBorSR4jTK/zWywKUlfjUftlEvWa4qqzKsSE0pyvrf629Ubir6awigcGnVEnP0IiZ5wjr4e
zjNiqr/IZ9IBl2eo6PU5BrITiUwg5p5yxcsOWqKUKXvOLE7kHEhQBbtU0/Ek4+p4NDnGZ7zh0FiJvpETJxKFhKx6Is6A
XxicGmYUJmvxjXmDTk+qzBSuZMxq0aUKTszlE6WhdM3FBkU5XZLCPT2l8UlHKOT1ubOBsqtnREzwI5G436TkSgk
xzYVkxr9bYbTDCFT/r0y9yshXUrRhlxRFG0sprxm2SY0q2/NYCrMGwkDAo6GZ/t+MCqhh/4/MVf2Pvv7DDMz/wP8Pg
/
+DyQEHyP+bUQE23P+JqD/zfxpZ9P5fewv8vwXo/d/W7OecjaRZhGWaZq04LtGUjCPIwkUQkrUXmI1xEstIUQmbOVD
/IdN/EyrAPfZ/Ff2z+v5P7RD03wpit+2TyoevQvtisv3jfJz48e1pxN3xs+1I74vpO89MxqurnY/XnlxeLFx702lcIjvurZ8ods/M
HQtevPD+bbBr+dR5amnN25XtflV+/fCLPbs62/fO+OD7yqzx9EzqbtfLk4GznxZurp+JHZ0+7l5+tPr8vtj2OfXr0sLKnHgrq
M6DAv9H/f/bCnCP/Z+ufzOm9PyfhfVfS9hvJkXsN4ci/iZ7gtkGAAAAAAAAAAAAAAAAAAAAAAAABAPX4DY
+BfEQB4AAA=
-- FIN DE L'ARCHIVE DE MESSAGE --

Appendice C. Exigences d'origine

Les exigences suivantes ont été dégagées d'après le développement du mécanisme décrit dans le présent document. Elles ont été conservées ici pour des raisons historiques.

- Le mécanisme doit permettre à un UAC ou à un serveur mandataire de fournir une forte assurance d'identité cryptographique dans une demande qui peut être par un serveur mandataire ou UAS.
- Les agents d'utilisateur qui reçoivent des assurances d'identité doivent être capables de valider ces assurances sans effectuer de recherches dans le réseau.
- Les agents d'utilisateur qui détiennent des certificats au nom de leur utilisateur doivent être capables d'ajouter cette assurance d'identité aux demandes.
- Les serveurs mandataires qui détiennent des certificats au nom de leur domaine doivent être capables d'ajouter cette assurance d'identité aux demandes ; un UAC n'est pas obligé de prendre en charge ce mécanisme afin qu'une assurance d'identité soit ajoutée à une demande de cette façon.
- Le mécanisme doit empêcher la répétition de l'assurance d'identité par un attaquant.
- Afin de fournir une pleine protection contre la répétition, le mécanisme doit être capable de protéger l'intégrité des corps

de message SIP (pour assurer que les offres et réponses de prend en charge sont liées à l'identité signalante).

- Il doit être possible à un utilisateur d'avoir plusieurs AoR (c'est-à-dire, comptes ou alias) qu'il est autorisé à utiliser au sein d'un domaine, et à l'UAC d'affirmer une identité tout en s'authentifiant comme une autre identité en rapport, comme permis par la politique locale du domaine.

9. Références

9.1 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)

[RFC2585] R. Housley et P. Hoffman, "Protocoles de fonctionnement de l'infrastructure de clé publique X.509 pour l'Internet : FTP et HTTP", mai 1999. *(P.S.)*

[RFC2818] E. Rescorla, "HTTP sur TLS", mai 2000. *(Information)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665, RFC8217)

[RFC3263] J. Rosenberg, H. Schulzrinne, "Protocole d'initialisation de session (SIP) : Localisation des serveurs SIP", juin 2002. (*Remplace* RFC2543) *(P.S. ; MàJ par* RFC7984)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3323] J. Peterson, "Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP)", novembre 2002.

[RFC3370] R. Housley, "Algorithmes de syntaxe de message cryptographique (CMS)", août 2002. *(P.S.)*

[RFC3548] S. Josefsson, "Codages de données Base16, Base32, et Base64", juillet 2003. *(Obsolète, voir* 4648) *(Info)*

[RFC3893] J. Peterson, "Format de corps d'identité authentifiée (AIB) du protocole d'initialisation de session (SIP)", septembre 2004.

[RFC4234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", octobre 2005. *(Remplace* RFC2234, *remplacée par* RFC5234)

9.2 Références pour information

[RFC3325] C. Jennings, J. Peterson et M. Watson, "Extensions privées au protocole d'initialisation de session (SIP) pour l'assertion d'identité au sein de réseaux de confiance", novembre 2002. *(Information ; ; MàJ par* RFC8217)

[RFC3761] P. Faltstrom, M. Mealling, "Application de E.164 au système de découverte dynamique de délégation (DDDS) d'identifiants de ressource uniformes (URI) (ENUM)", avril 2004. *(P.S.) (Obsolète, voir la* RFC6116)

[RFC3966] H. Schulzrinne, "L'URI tel pour les numéros de téléphone", décembre 2004. (*MàJ par* RFC5341) *(P.S.)*

[RFC4475] R. Sparks et autres, "Messages d'essais de résistance du protocole d'initialisation de session (SIP)", mai 2006. *(Info.)*

[15] Peterson, J., "Retargeting and Security in SIP: A Framework and Requirements", Travail en cours, février 2005.

Adresse des auteurs

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
US
téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz
URI : http://www.neustar.biz/

Cullen Jennings
Cisco Systems
170 West Tasman Drive
MS: SJC-21/2
San Jose, CA 95134
US
téléphone : +1 408 902-3341
mél : fluffy@cisco.com

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2006).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle
L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.