Groupe de travail Réseau
Request for Comments : 3324
Catégorie : Information

M. Watson, Nortel Networks
novembre 2002
Traduction Claude Brière de L'Isle

Exigences à court terme pour l'identité attestée par le réseau

Résumé
Une identité attestée par le réseau est une identité déduite initialement par un intermédiaire réseau du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) suite à un processus d'authentification. Le présent document décrit les exigences à court terme pour l'échange des identités attestées par le réseau au sein de réseaux constitués de nœuds interconnectés de façon sécurisée et avec des agents d'utilisateur connectés de façon sécurisée à de tels réseaux.

Il n'y a pas d'exigence que l'identité attestée par un agent d'utilisateur dans un message SIP soit autre chose que l'alias désiré de l'utilisateur.

Table des matières

1. Introduction....1
2. Définitions....2
  2.1 Identité....2
  2.2 Identité attestée par le réseau....2
  2.3 Domaines de confiance....2
  2.4 Spec(T)....4
3. Génération de l'identité attestée par le réseau....4
4. Transport de l'identité attestée par le réseau....4
  4.1 Envoi d'une identité attestée par le réseau dans un domaine de confiance....4
  4.2 Réception d'une identité attestée par le réseau dans un domaine de confiance....4
  4.3 Envoi d'une identité attestée par le réseau en dehors d'un domaine de confiance....4
  4.4 Réception d'une identité attestée par le réseau en dehors d'un domaine de confiance....4
5. Parties à l'identité attestée par le réseau....5
6. Types d'identité attestée par le réseau....5
7. Confidentialité de l'identité attestée par le réseau....5
8. Considérations pour la sécurité....5
9. Considérations relatives à l'IANA....6
10. Remerciements....6
Référence normative....6
Déclaration complète de droits de reproduction....6

1. Introduction

SIP [1] permet aux usagers d'attester de leur identité d'un certain nombre de façons, par exemple, en utilisant l'en-tête From:. Cependant, il n'y a pas d'exigence que ces identités soient autre chose que les pseudonymes désirés par l'usager.

Une identité authentifiée d'un usager peut être obtenue en utilisant l'authentification SIP par résumé (ou par d'autres moyens). Cependant, les agents d'utilisateur n'ont pas toujours les informations clés nécessaires pour authentifier un autre agent d'utilisateur (UA, *user agent*).

Une identité attestée par le réseau est une identité déduite initialement par un intermédiaire de réseau SIP par suite d'un processus d'authentification. Cela peut être ou non fondé sur l'authentification SIP par résumé. Le présent document décrit les exigences de court terme pour l'échange des identités attestées par le réseau au sein de réseaux de nœuds de confiance interconnectés de façon sûre et aussi pour les agents d'utilisateur qui ont des connexions sécurisées avec de tels réseaux.

Un tel réseau est décrit dans le présent document comme un domaine de confiance, et on présente une définition stricte de la confiance et du domaine de confiance dans le cadre du présent document. Ces exigences de court terme ne valent que pour l'échange des identités attestées par le réseau au sein d'un domaine de confiance et envers une entité directement connectée au domaine de confiance.

Les exigences générales pour le transport des identités attestées par le réseau sur l'Internet sortent du domaine d'application du présent document.

2. Définitions

2.1 Identité

Une identité, pour les besoins du présent document, est un URI sip:, sips: ou tel:, et facultativement un nom d'affichage.

L'URI DOIT avoir une signification dans le domaine identifié dans l'URI (dans le cas des URI sip: ou sips:) ou chez le possesseur du numéro E.164 (dans le cas des URI tel:), au sens qu'utilisée comme URI de demande SIP dans une demande envoyée à ce possesseur de gamme de domaine/numéro, elle cause l'acheminement de la demande à l'usager/ligne associé à cette identité, ou soit traitée par le logiciel de service qui fonctionne au nom de cet usager.

Si l'URI est un URI sip: ou sips:, selon la politique locale du domaine identifié dans l'URI, celui-ci PEUT alors identifier une entité spécifique, telle qu'une personne.

Si l'URI est un URI tel:, selon la politique locale du possesseur de la gamme de numéros au sein de laquelle se situe le numéro de téléphone, le numéro PEUT identifier une entité spécifique, comme une ligne téléphonique. Cependant, il vaut de noter que l'identification du possesseur de la gamme de numéros est un processus moins direct que l'identification du domaine qui détient un URI sip: ou sips:.

2.2 Identité attestée par le réseau

Une identité attestée par le réseau est une identité déduite par une entité de réseau SIP par suite d'un processus d'authentification, qui identifie l'entité authentifiée au sens défini au paragraphe 2.1.

Dans le cas d'un URI sip: ou sips:, le domaine inclus dans l'URI DOIT être au sein du domaine de confiance.

Dans le cas d'un URI tel:, le possesseur du numéro E.164 qui est dans l'URI DOIT être au sein du domaine de confiance.

Le processus d'authentification utilisé, ou au moins sa fiabilité/force, est une caractéristique connue du domaine de confiance qui utilise le mécanisme d'identité attestée par le réseau, c'est-à-dire, dans le langage du paragraphe 2.3 ci-dessous, elle est définie dans une Spec(T).

2.3 Domaines de confiance

Pour les besoins de l'identité attestée par le réseau, un domaine de confiance est un ensemble de nœuds SIP (UAC, UAS, mandataires ou autres intermédiaires du réseau) qui sont de confiance pour l'échange des informations d'identité attestée par le réseau au sens décrit ci-dessous.

Un nœud peut être membre d'un domaine de confiance T si et seulement si le nœud est connu comme conforme à un ensemble de spécifications, Spec(T), qui caractérisent le traitement de l'identité attestée par le réseau au sein du domaine de confiance T.

Les domaines de confiance sont construits par des personnes qui connaissent les propriétés des équipements qui sont utilisés/déployés. Dans le cas le plus simple, un domaine de confiance est un ensemble d'appareils dont un seul possesseur/opérateur peut réellement connaître le comportement.

De tels domaines de confiance simples peuvent être rassemblés en plus grands domaines de confiance par des accords bilatéraux entre les propriétaires/opérateurs des appareils.

On dit d'un nœud qu'il est 'de confiance' (par rapport à un domaine de confiance donné) si et seulement si il est un membre de ce domaine.

On dit qu'un nœud A, dans le domaine, est "de confiance" pour un nœud B (ou que 'B fait confiance à A') si et seulement si :
1. il y a une connexion sécurisée entre les nœuds, ET
2. B a des informations de configuration qui indiquent que A est membre du domaine de confiance.

Noter que B peut être ou non membre du domaine de confiance. Par exemple, B peut être un agent d'utilisateur qui fait confiance à un intermédiaire réseau donné A (par exemple, son mandataire de rattachement).

Une "connexion sécurisée" dans ce contexte signifie que les messages ne peuvent pas être lus par des tiers, ne peuvent pas être modifiés par des tiers sans détection et que B peut être sûr que le message vient bien de A. Le niveau de sécurité exigé est une caractéristique du domaine de confiance, c'est-à-dire, il est défini dans la Spec(T).

Dans ce contexte, les informations de signalisation SIP reçues par un nœud DE LA PART d'un nœud de confiance sont connues pour avoir été générées et transmises à travers le réseau conformément aux procédures de l'ensemble de spécification Spec(T) particulier, et donc sont réputées valides, ou au moins aussi valides que spécifié dans les spécifications Spec(T).

Également, un nœud peut être sûr que les informations de signalisation passées VERS un nœud qui est de confiance seront traitées conformément aux procédures de Spec(T).

Pour que ces capacités soient utiles, Spec(T) doit contenir les exigences sur la façon dont l'identité attestée par le réseau est générée, la façon dont la confidentialité est protégée, et comment son intégrité est conservée lors de son passage à travers le réseau. Un lecteur de Spec(T) peut avoir un jugement argumenté sur l'authenticité et la fiabilité des informations attestées par le réseau reçues du domaine de confiance T.

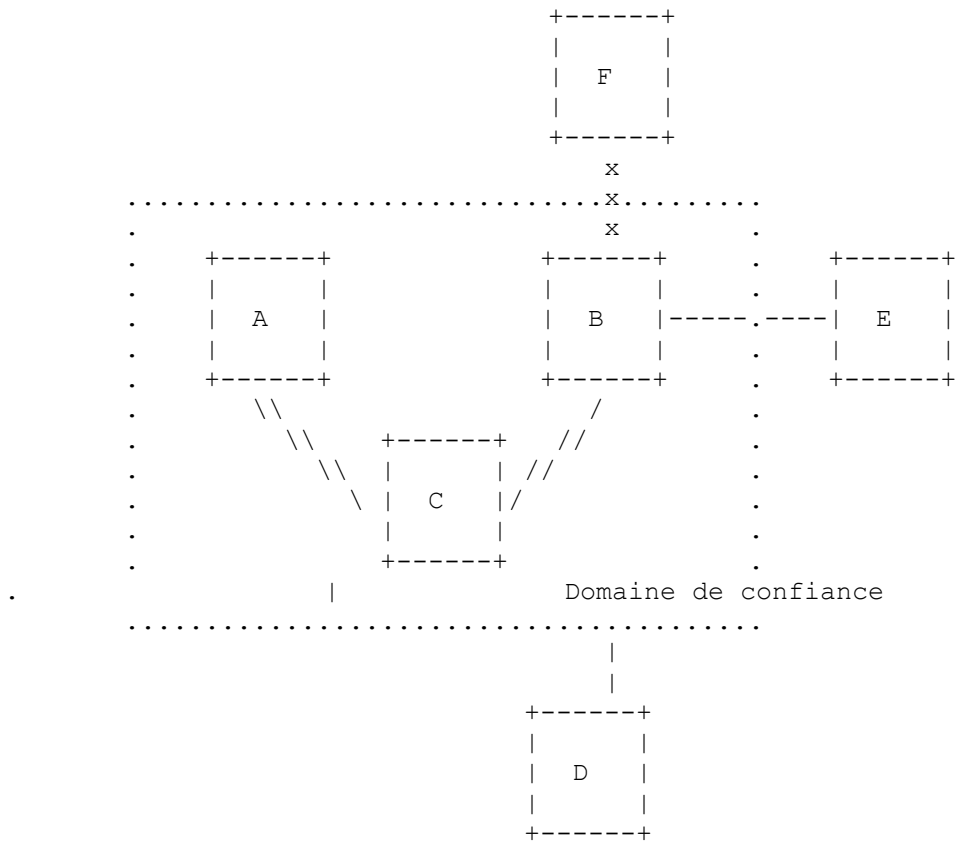
Le terme "de confiance" (par rapport à un domaine de confiance donné) peut s'appliquer à un nœud donné dans un sens absolu – c'est exactement équivalent à dire que le nœud est membre du domaine de confiance. Cependant, le nœud lui-même ne sait pas si un autre nœud quelconque est "de confiance", même au sein du domaine de confiance. Il le sait de certains nœuds avec lesquels il a des connexions sécurisées comme décrit ci-dessus.

Avec la définition ci-dessus, des déclarations telles que "un nœud de confiance DEVRA" sont un simple raccourci pour "un nœud conforme à la présente spécification DEVRA..."

Des déclarations telles que "lorsqu'un nœud reçoit des informations d'un nœud de confiance..." NE SONT PAS valides, parce que un nœud n'a pas une connaissance complète des autres nœuds du domaine de confiance.

Des déclarations telles que "lorsque un nœud reçoit des informations d'un autre nœud qui est pour lui de confiance...' SONT valides, et doivent être interprétées conformément aux critères (1) et (2) ci-dessus.

Les relations ci-dessus sont illustrées par la figure suivante.



xxxxxx Connexion non sûre
-------- Connexion sûre
..... . Toutes les boîtes à l'intérieur des pointillés font partie du même domaine de confiance

- o A, B et C font partie du même domaine de confiance
- o A fait confiance à C, mais A ne fait pas confiance à B
- o Comme E sait que B est dans le domaine de confiance, E fait confiance à B, mais B ne fait pas confiance à E
- o B ne fait pas confiance à F, F ne fait pas confiance à B

2.4 Spec(T)

Un aspect de la définition d'un domaine de confiance est que tous les éléments dans ce domaine sont conformes à un ensemble de configurations et spécifications qu'on appelle généralement Spec(T). Spec(T) n'est pas une spécification au sens d'un document écrit ; c'est plutôt un accord sur un ensemble d'informations que tous les éléments connaissent. Le traitement approprié des identités attestées exige que les éléments sachent ce qui est réellement attesté, comment cela a été déterminé, et ce que sont les politiques de confidentialité. Toutes ces informations sont caractérisées par la Spec(T).

3. Génération de l'identité attestée par le réseau

Une identité attestée par le réseau est générée par un intermédiaire réseau suivant un processus d'authentification qui authentifie l'entité (UA) à identifier.

Le ou les processus d'authentification utilisés sont une caractéristique du domaine de confiance, et DOIVENT être spécifiés dans la Spec(T).

Il devra être possible à un agent d'utilisateur de fournir une identité préférée à l'intermédiaire réseau, qui PEUT être utilisé pour informer de la génération de l'identité attestée par le réseau conformément aux politiques du domaine de confiance.

4. Transport de l'identité attestée par le réseau

4.1 Envoi d'une identité attestée par le réseau dans un domaine de confiance

Il devra être possible à un nœud au sein d'un domaine de confiance d'envoyer de façon sécurisée une identité attestée par le réseau à un autre nœud de confiance.

4.2 Réception d'une identité attestée par le réseau dans un domaine de confiance

Il devra être possible à un nœud au sein d'un domaine de confiance de recevoir une identité attestée par le réseau d'un autre nœud de confiance.

4.3 Envoi d'une identité attestée par le réseau en dehors d'un domaine de confiance

Si un nœud A, au sein du domaine de confiance, est de confiance pour un nœud B, en dehors du domaine de confiance, il devra alors être possible à A d'envoyer en toute sécurité une identité attestée par le réseau pour B, si cela est permis par les politiques de confidentialité de l'usager qui a été identifié, et celle du domaine de confiance.

Ceci est utilisé le plus souvent pour passer directement une identité attestée par le réseau à un agent d'utilisateur.

4.4 Réception d'une identité attestée par le réseau en dehors d'un domaine de confiance

Il devra être possible à un nœud en dehors du domaine de confiance de recevoir une identité attestée par le réseau provenant d'un nœud de confiance.

L'identité attestée par le réseau reçue de cette façon peut être considérée comme valide, et utilisée pour l'afficher à l'usager, pour des entrées de données pour des services, etc.

Les informations d'identité attestée par le réseau reçues par un nœud en provenance d'un nœud qui n'est pas de confiance ne portent aucune garantie d'authenticité ou d'intégrité parce qu'on ne sait pas si les procédures de Spec(T) ont été suivies pour générer et transporter les informations. De telles informations NE DOIVENT PAS être utilisées. (C'est-à-dire, elle ne devront pas être affichées à l'usager, être passées aux autres nœuds, utilisées comme données d'entrées pour des services, etc.)

5. Parties à l'identité attestée par le réseau

Une identité attestée par le réseau identifie l'origine du message dans lequel elle a été reçue.

Par exemple,

- une identité attestée par le réseau reçue dans une INVITE initiale (en dehors du contexte de tout dialogue existant) identifie l'appelant.

- une identité attestée par le réseau reçue dans une réponse 180 Sonnerie à une telle INVITE identifie la partie qui sonne.

- une identité attestée par le réseau reçue dans une réponse 200 à une telle INVITE identifie la partie qui a répondu.

6. Types d'identité attestée par le réseau

Il devra être possible d'attester plusieurs identités associées à une certaine partie (dans un message donné) pourvu qu'elles soient de types distincts.

Les types d'identité acceptés devront être des URI sip:, sips: et tel:, dont toutes identifient l'usager comme décrit au paragraphe 2.1. Il n'est pas exigé de transporter les deux URI sip: et sips:.

Il devra être possible d'avoir la capacité à transporter des types d'identité supplémentaires associés à une seule partie qui sera introduite à l'avenir.

7. Confidentialité de l'identité attestée par le réseau

Le moyen par lequel est déterminée une exigence de confidentialité par rapport à l'identité attestée par le réseau sort du domaine d'application du présent document.

Il devra être possible d'indiquer au sein d'un message contenant une identité attestée par le réseau que cette identité attestée par le réseau est soumise à une exigence de confidentialité qui empêche de la passer aux autres usagers. Cette indication ne devrait porter aucune sémantique relative à la raison de cette exigence de confidentialité.

Il devra être possible d'indiquer que l'usager a demandé que l'identité attestée par le réseau ne soit pas passée aux autres usagers. Ceci est distinct de l'indication précédente, en ce qu'elle implique une intention spécifique de l'usager par rapport à l'identité attestée par le réseau.
Le mécanisme devra prendre en charge les politiques de domaine de confiance où les deux indications ci-dessus sont équivalentes (c'est-à-dire que la seule raison possible pour une exigence de confidentialité est une demande de l'usager) et les politiques où elles ne le sont pas.

Dans ce cas, la spécification de l'identité attestée par le réseau devra exiger que le mécanisme du paragraphe 4.3 NE SERA PAS utilisé, c'est-à-dire qu'un nœud de confiance ne devra pas passer l'identité à un nœud qui n'est pas de confiance. Cependant, le mécanisme du paragraphe 4.3 PEUT être utilisé pour transférer l'identité au sein du réseau de confiance.

Noter que les demandes "anonymat" de la part des usagers ou abonnées peuvent exiger des fonctionnalités qui s'ajoutent au traitement ci-dessus des identités attestées par le réseau . De telles fonctionnalités supplémentaires sortent du domaine d'application du présent document.

8. Considérations pour la sécurité

Les exigences du présent document NE SONT PAS destinées à aboutir à un mécanisme d'application générale entre des hôtes arbitraires sur l'Internet.

L'intention est plutôt de déclarer les exigences pour un mécanisme à utiliser au sein d'une communauté d'appareils qui sont connus pour obéir à la spécification du mécanisme Spec(T) et entre lesquels existent des connexions sécurisées. Une telle communauté est appelées ici un domaine de confiance.

Les exigences pesant sur les mécanismes utilisés pour la sécurité et pour déduire initialement une identité attestée par le réseau doivent figurer dans la spécification Spec(T).

Les exigences prennent aussi en charge le transfert des informations provenant d'un nœud à l'intérieur du domaine de confiance, via une connexion sécurisée, vers un nœud en dehors du domaine de confiance.

L'utilisation de ce mécanisme dans tout autre contexte présente de sérieux inconvénients pour la sécurité, à savoir qu'il n'y a absolument aucune garantie que les informations n'ont pas été modifiées, ou étaient même correctes au départ.

9. Considérations relatives à l'IANA

Le présent document n'a aucune implication pour l'IANA.

10. Remerciements

Des remerciements sont dus à Jon Peterson, Cullen Jennings, Allison Mankin et Jonathan Rosenberg pour leurs commentaires sur le présent document.

Référence normative

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley et E. Schooler, "SIP : Protocole d'initialisation de session", RFC 3261, juin 2002.

Adresse de l'auteur

Mark Watson
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead, BERKS SL6 3QH
UK
mél : mwatson@nortelnetworks.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.