Groupe de travail Réseau
Request for Comments : 3182
RFC rendue obsolète : 2752
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Yadav, R. Yavatkar, Intel
R. Pabbati, P. Ford, T. Moore, Microsoft
S. Herzog, PolicyConsulting.Com
R. Hess, Intel
octobre 2001

Représentation d'identité pour RSVP

Résumé
Le présent document décrit la représentation des informations d'identité dans l'objet POLICY_DATA pour la prise en charge du contrôle d'admission fondé sur la politique dans le protocole de réservation de ressource (RSVP). Le but de la représentation d'identité est de permettre à un processus sur un système d'identifier en toute sécurité le propriétaire et l'application du processus de communication (par exemple, l'identifiant d'utilisateur) et de porter ces informations dans les messages RSVP (PATH ou RESV) d'une manière sûre. On décrit le codage des identités comme élément de politique RSVP. On décrit les règles de traitement pour générer les éléments de politique d'identification pour les flux fusionnés de diffusion groupée. On décrit ensuite les représentations des identités d'utilisateur pour Kerberos et les mécanismes d'authentification fondés sur les clés publiques. En résumé, on décrit l'utilisation de ces informations d'identité dans un ensemble opérationnel.

Le présent mémoire corrige une erreur d'allocation de codet RSVP P-Type POLICY_DATA et une erreur de la définition de la taille d'un champ dans la valeur d'erreur de la [RFC2752].

Table des matières

1. Conventions utilisées dans ce document

Dans le présent document, les mots clé "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRAIT" NE DEVRAIT PAS", "RECOMMANDÉ", "NON RECOMMANDÉ", "PEUT", et "FACULTATIF" doivent être interprétés comme décrit dans le BCP 14, [RFC2119]

2. Introduction

RSVP [RFC2205] est un protocole de réservation de ressources conçu pour un Internet à intégration de services [RFC1633]. RSVP est utilisé par un hôte pour demander une qualité de service (QS) spécifique de la part du réseau pour des flux de données d'application particuliers. RSVP est aussi utilisé par les routeurs pour livrer des demandes de QS à tous les nœuds le long du ou des chemins des flux et pour établir et maintenir l'état destiné à fournir le service demandé. Les demandes RSVP vont généralement résulter en ressources réservées dans chaque nœud le long du chemin des données. RSVP permet à des utilisateurs particuliers d'obtenir un accès préférentiel aux ressources du réseau, sous la supervision d'un mécanisme de contrôle d'admission. La permission de faire une réservation se fonde à la fois sur la disponibilité des ressources demandées le long du chemin des données et sur la satisfaction à des règles de politique. La fourniture d'un mécanisme de contrôle d'admission fondé sur une politique sur la base de l'identité de l'utilisateur est une des principales exigences.

Afin de résoudre ces problèmes et mettre en œuvre un contrôle de politique fondé sur l'identité, il est nécessaire d'identifier l'utilisateur et/ou l'application qui fait une demande RSVP.

Le présent document propose un mécanisme pour l'envoi des informations d'identification dans les messages RSVP et permet des décisions d'autorisation sur la base de la politique et de l'identité.

On décrit l'élément de politique d'authentification (AUTH_DATA) contenu dans l'objet POLICY_DATA. Le processus d'utilisateur peut générer un élément de politique AUTH_DATA et le donner au processus RSVP (service) sur l'hôte d'origine. Le service RSVP insère AUTH_DATA dans le message RSVP pour identifier le propriétaire (utilisateur et/ou application) qui fait la demande de ressources réseau. Les éléments de réseau, tels que les routeurs, authentifient la demande en utilisant les accréditifs présentés dans AUTH_DATA et admettent le message RSVP sur la base de la politique d'admission. Après l'authentification d'une demande, le routeur de premier bond installe l'état RSVP et transmet le nouvel élément de politique retourné par le point de décision de politique (PDP, *Policy Decision Point*) [RFC2753].

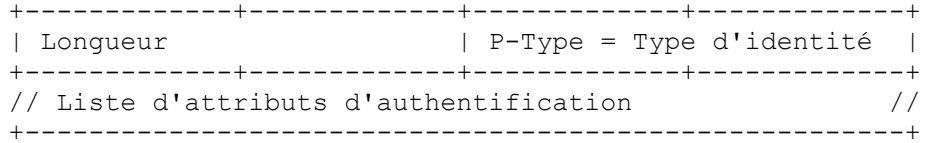
3. Élément de politique pour les données d'authentification

3.1 Format d'objet de données de politique

Les objets POLICY_DATA contiennent des informations de politique et sont portés par les messages RSVP. Une description détaillée du format de l'objet POLICY_DATA se trouve dans la [RFC2750] "Extensions RSVP pour le contrôle de politique".

3.2 Élément de politique de données d'authentification

Dans ce paragraphe, on décrit un élément de politique (PE) appelé données d'authentification (AUTH_DATA). L'élément de politique AUTH_DATA contient une liste d'attributs d'authentification .



Longueur
C'est la longueur de l'élément de politique (incluant Longueur et P-Type) en nombre d'octets (DOIT être un multiple de 4) et indique la fin de la liste d'attributs d'authentification.

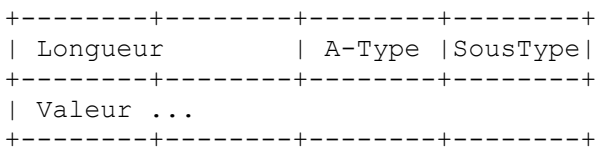
P-Type (Type d'identité)
Ce sont les informations de type d'identité contenues dans cet élément de politique fourni comme type d'élément de politique (P-type). L'autorité d'allocation des numéros de l'Internet (IANA) agit comme registraire pour les types d'éléments de politique pour l'identité, comme décrit dans la [RFC2750]. Initialement, le registre contient les P-Types suivants pour l'identité :

2	AUTH_USER	Schéma d'authentification pour identifier les utilisateurs
3	AUTH_APP	Schéma d'authentification pour identifier les applications

Liste des attributs d'authentification
Les attributs d'authentification contiennent des informations spécifiques de la méthode et du type d'authentification de AUTH_DATA. L'élément de politique fournit le mécanisme pour grouper une collection d'attributs d'authentification.

3.3 Attributs d'authentification

Les attributs d'authentification DOIVENT être codés comme multiples de 4 octets ; les attributs qui ne sont pas des multiples de 4 octets DOIVENT être bourrés jusqu'à une frontière de 4 octets.



Longueur
Le champ Longueur fait deux octets et indique la longueur réelle de l'attribut (y compris les champs Longueur et A-Type) en nombre d'octets. La longueur n'inclut aucun des octets de bourrage du champ de valeur pour faire de l'attribut un multiple de 4 octets.

A-Type
Le champ Type d'attribut f'authentification (A-Type) fait un octet. L'IANA est le registraire des A-Types comme décrit dans la section 8, Considérations relatives à l'IANA. Au départ, le registre contient les A-Types suivants :

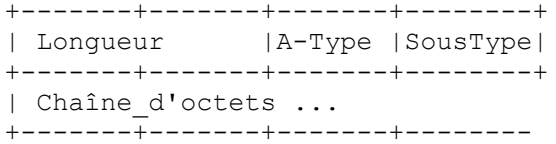
1	LOCALISATEUR_DE_POLITIQUE	Chaîne unique pour localiser la politique d'admission (comme le DN X.500 décrit dans la [RFC1779]).
2	ACCREDITIF	Accréditif de l'usager comme un ticket Kerberos ou un certificat numérique. Accréditif de l'application comme un identifiant d'application.
3	SIGNATURE_NUMERIQUE	Signature numérique de l'élément de politique de données d'authentification.
4	OBJET_ERREUR_POLITIQUE	Informations détaillées sur les défaillances de politique.

SousType
Le champ Soustype d'attribut d'authentification fait un octet. La valeur de SousType dépend du A-type.

Valeur
Le champ Valeur contient les informations spécifiques de l'attribut.

3.3.1 Localisateur de politique

LOCALISATEUR_DE_POLITIQUE est utilisé pour localiser la politique d'admission pour l'usager ou l'application. Le nom distinctif (DN, *Distinguished Name*) est unique pour chaque usager ou application, donc un DN est utilisé comme localisateur de politique.



Longueur
Longueur de l'attribut, qui DOIT être ≥ 4.

A-Type
LOCALISATEUR_DE_POLITIQUE

SousType
Les sous-types suivants sont définis pour LOCALISATEUR_DE_POLITIQUE. L'IANA est le registraire des sous-types de LOCALISATEUR_DE_POLITIQUE, comme décrit dans la section 8, sur les considérations relatives à l'IANA. Au départ, le registre contient les sous-types suivants pour LOCALISATEUR_DE_POLITIQUE :

1	ASCII_DN	Chaîne_d'octets contient le DN X.500 décrit dans la RFC1779 comme chaîne ASCII.
2	UNICODE_DN	Chaîne_d'octets contient le DN X.500 décrit dans la RFC1779 comme chaîne UNICODE.
3	ASCII_DN_ENCRYPT	Chaîne_d'octets contient le DN X.500 chiffré. La clé de session Kerberos ou la clé privée de certificat numérique est utilisée pour le chiffrement. Pour le chiffrement Kerberos, le format est le même que celui retourné de gss_seal [RFC1509].
4	UNICODE_DN_ENCRYPT	Chaîne_d'octets contient le DN X.500 chiffré UNICODE. La clé de session Kerberos ou la clé privée de certificat numérique est utilisée pour le chiffrement. Pour le chiffrement Kerberos, le format est le même que celui retourné de gss_seal [RFC1509].

Chaîne_d'octets
Le champ Chaîne_d'octets contient le nom distinctif (DN).

3.3.2 Accréditif

ACCRÉDITIF indique l'accréditif de l'usager ou application à authentifier. Pour la méthode d'authentification Kerberos, l'objet ACCRÉDITIF contient le ticket de session Kerberos. Pour l'authentification fondé sur une clé publique, ce champ contient un certificat numérique.

Un résumé du format de l'attribut ACCRÉDITIF figure ci-dessous. Les champs sont transmis de gauche à droite.

```
+-------+-------+-------+--------+
| Longueur      |A-Type |SousType|
+-------+-------+-------+--------+
| Chaîne_d'octet ...
+-------+-------+-------+--------
```

Longueur
Longueur de l'attribut, qui DOIT être ≥ 4.

A-Type
ACCREDITIF

SousType
L'IANA est le registraire des sous-types ACCREDITIF comme décrit à la section 8, sur les considérations relatives à l'IANA. Au départ, le registre contient les sous-types suivants pour ACCREDITIF :

1	ASCII_ID	Chaîne_d'octet contient l'identification d'usager ou d'application en une chaîne de texte entièrement ASCII.
2	UNICODE_ID	Chaîne_d'octet contient l'identification d'usager ou d'application en une chaîne de texte entièrement en UNICODE.
3	KERBEROS_TKT	Chaîne_d'octet contient un ticket Kerberos.
4	X509_V3_CERT	Chaîne_d'octet contient un certificat numérique X.509 V3 [RFC2459].
5	PGP_CERT	Chaîne_d'octet contient un certificat numérique PGP.

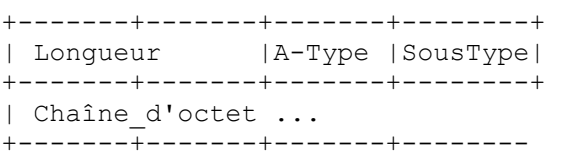
Chaîne_d'octet
La chaîne d'octet contient l'accréditif de l'usager ou de l'application.

3.3.3 Signature numérique

L'attribut SIGNATURE_NUMÉRIQUE DOIT être le dernier attribut dans la liste des attributs et contient la signature numérique de l'élément de politique AUTH_DATA. La signature numérique signe toutes les données dans l'élément de

politique AUTH_DATA jusqu'à la signature numérique. L'algorithme utilisé pour calculer la signature numérique dépend de la méthode d'authentification spécifiée par le champ de sous-type ACCREDITIF.

Un résumé du format de l'attribut SIGNATURE_NUMÉRIQUE figure ci-dessous.



Longueur
Longueur de l'attribut, qui DOIT être ≥ 4.

A-Type
SIGNATURE_NUMÉRIQUE

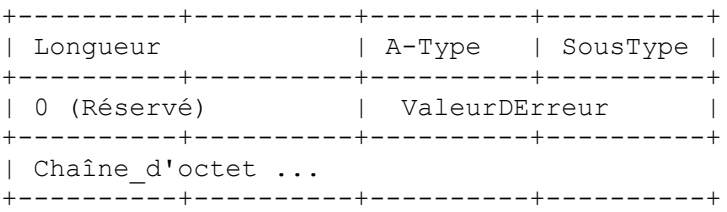
SousType
Aucun sous-type n'est actuellement défini pour SIGNATURE_NUMÉRIQUE. Ce champ DOIT être réglé à 0.

Chaîne_d'octet
Chaîne_d'octet contient la signature numérique de AUTH_DATA.

3.3.4 Objet Erreur de politique

Cet attribut est utilisé pour porter toutes les erreurs spécifiques du contrôle de politique générées par un nœud lors du traitement/validation d'un élément de politique de données d'authentification. Lorsque un nœud de politique RSVP (point de décision de politique local ou PDP distant) rencontre une demande qui échoue aux contrôles de politique du fait de son élément de politique d'authentification, il DOIT ajouter un CODE_D'ERREUR_DE_POLITIQUE contenant des informations supplémentaires sur la raison de la défaillance survenue dans l'élément de politique. Cela va alors causer un message ERREUR_DE_CHEMIN ou ERREUR_DE_RESV approprié généré à l'élément de politique et un code d'erreur RSVP approprié dans le message, qui est retourné à la source de la demande.

L'élément de politique AUTH_DATA dans le message PATH ou RSVP NE DEVRAIT PAS contenir l'attribut OBJET_ERREUR_DE_POLITIQUE. Celui-ci n'est inséré dans les messages ERREUR_DE_CHEMIN et ERREUR_RESV que lorsque ils sont générés par des nœuds intermédiaires à capacité politique.



Longueur
Longueur de l'attribut, qui DOIT être ≥ 8.

A-Type
CODE_D'ERREUR_DE_POLITIQUE

SousType
Aucun sous-type n'est actuellement défini pour CODE_D'ERREUR_DE_POLITIQUE. Ce champ DOIT être réglé à 0.

ValeurDErreur
C'est un code de 16 bits qui contient la raison de la défaillance de ce point de décision de politique à traiter l'élément de politique. L'IANA est le registraire pour les valeurs d'erreur, comme décrit à la section 8, sur les considérations relatives à l'IANA. Les valeurs suivantes ont été définies :

1	PAS_D'INFO_D'ERREUR	Aucune information n'est disponible.
2	TYPE_D'ACCREDITIF_NON_ACCEPTE	Ce type d'accréditif n'est pas accepté.
3	PRIVILEGE_INSUFFISANT	Les accréditifs n'ont pas de privilège suffisant.
4	ACCREDITIF_EXPIRE	L'accréditif est arrivé à expiration.
5	IDENTITÉ_CHANGÉE	L'identité a changé.

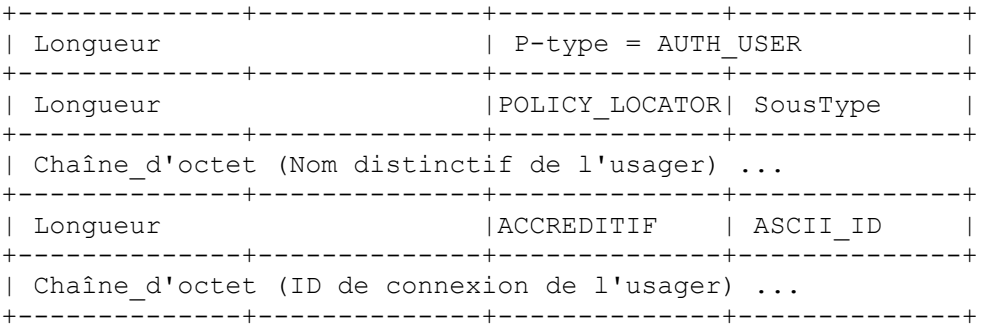
Chaîne_d'octets
Le champ Chaîne_d'octets contient des informations provenant du point de décision de politique qui PEUVENT contenir des informations supplémentaires sur la défaillance de politique. Par exemple, il peut comporter un message lisible par l'homme dans le texte ASCII.

4. Formats des données d'authentification

Les attributs d'authentification sont groupés en un élément de politique pour représenter les accréditifs d'identité.

4.1 Authentification simple d'utilisateur

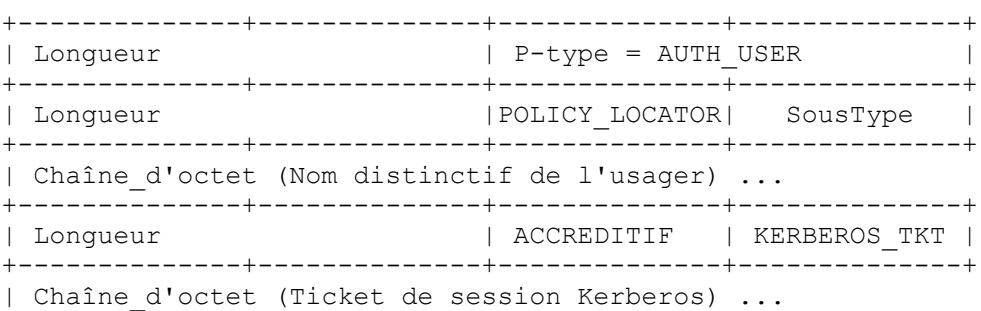
Dans la méthode simple d'authentification d'utilisateur, l'identifiant de connexion (en texte ASCII ou UNICODE clair) est codé comme un attribut ACCREDITIF. Un résumé du format de l'élément de politique de simple utilisateur AUTH_DATA est montré ci-dessous.



4.2 Authentification d'utilisateur Kerberos

L'authentification Kerberos [RFC1510] utilise un tiers de confiance (le centre de distribution Kerberos (KDC)) pour pourvoir à l'authentification de l'usager auprès d'un serveur réseau. On suppose qu'un KDC est présent et que l'hôte et le vérificateur des informations d'authentification (routeur ou PDP) mettent en œuvre l'authentification Kerberos.

Un résumé de l'élément de politique Kerberos AUTH_DATA figure ci-dessous.

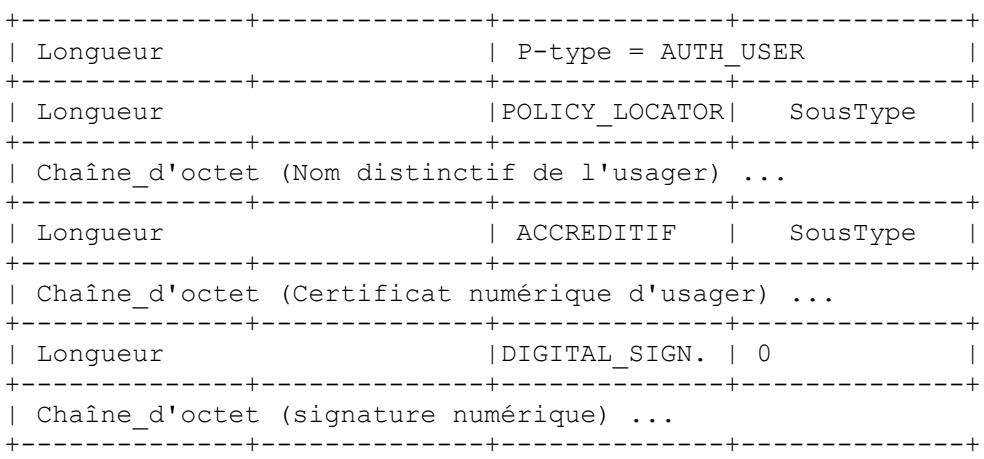


4.2.1 Réglage du fonctionnement avec des identités Kerberos

Un hôte à capacité RSVP est configuré pour construire et insérer un élément de politique AUTH_DATA dans les messages RSVP qui désignent l'utilisation de la méthode d'authentification Kerberos (KERBEROS_TKT). À l'initialisation de la session RSVP, l'application d'utilisateur contacte le KDC pour obtenir un ticket Kerberos pour le prochain nœud de réseau ou son PDP. Un routeur lorsqu'il génère un message RSVP contacte le KDC pour obtenir un ticket Kerberos pour le nœud de réseau du prochain bond ou son PDP. L'identité du PDP ou du prochain bond de réseau peut être configurée de façon statique, apprise via DHCP ou conservée dans un service de répertoire. Le ticket Kerberos est envoyé au prochain nœud de réseau (qui peut être un routeur ou un hôte) dans un message RSVP. Le KDC est utilisé pour valider le ticket et authentifier l'usager qui envoie le message RSVP.

4.3 Authentification d'utilisateur fondée sur une clé publique

Dans la méthode d'authentification d'utilisateur fondée sur la clé publique, le certificat numérique est codé comme les accréditifs d'usager. La signature numérique est utilisée pour authentifier l'usager. Un résumé de l'élément de politique AUTH_DATA de l'utilisateur de la clé publique est montré ci-dessous.



4.3.1 Réglage du fonctionnement pour l'authentification fondée sur la clé publique

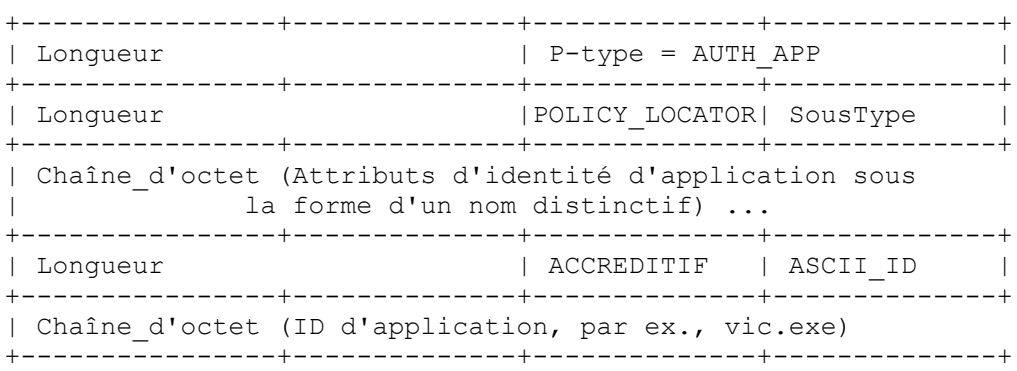
L'authentification fondée sur la clé publique suppose ce qui suit :

- les demandeurs de service RSVP ont une paire de clés (clé privée et clé publique),
- la clé privée est sécurisée par l'usager,
- les clés publiques sont mémorisées dans des certificats numériques et un tiers de confiance , l'autorité de certificat (CA) produit ces certificats numériques,
- le vérificateur (PDP ou routeur) a la capacité de vérifier le certificat numérique.

Le demandeur RSVP utilise sa clé privée pour générer la SIGNATURE_NUMERIQUE. Les authentificateurs de l'usager (routeur, PDP) utilisent la clé publique de l'usager (mémorisée dans le certificat numérique) pour vérifier la signature et authentifier l'usager.

4.4 Authentification simple d'application

La méthode d'authentification d'application code l'identification d'application telle qu'un nom de fichier exécutable comme du texte ASCII ou UNICODE en clair.



5. Fonctionnement

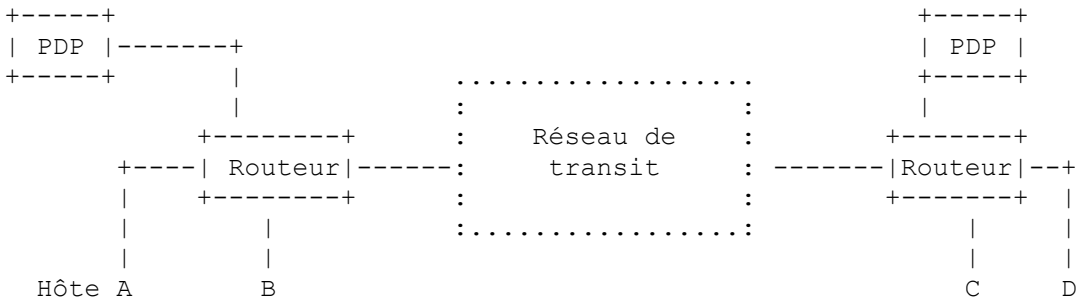


Figure 1 : Authentification d'usager et d'application avec le PE AUTH_DATA

Les nœuds de réseau (hôtes/routeurs) génèrent des éléments de politique (PE, *policy element*) AUTH_DATA, dont les contenus dépendent du type d'identité utilisé et de la méthode d'authentification utilisée. Ils contiennent généralement des accréditifs d'authentification (ticket Kerberos ou certificat numérique) et des localisateurs de politique (qui peuvent être le nom distinctif X.500 de l'usager ou du nœud de réseau, ou des noms d'application). Les nœuds de réseau génèrent un élément de politique AUTH_DATA qui contient l'identité d'authentification lorsque on fait la demande RSVP ou lors de la transmission d'un message RSVP.

Les nœuds de réseau génèrent l'élément de politique AUTH_DATA d'usager en utilisant les règles suivantes :

1. Pour les sessions en envoi individuel, le localisateur de politique d'utilisateur est copié du bond précédent. Les accréditifs d'authentification sont pour l'identité du nœud de réseau actuel.
2. Pour les messages en diffusion groupée, le localisateur de politique d'utilisateur est pour l'identité du nœud de réseau en cours. Les accréditifs d'authentification sont pour le nœud de réseau actuel.

Les nœuds de réseau génèrent un élément de politique AUTH_DATA d'application en utilisant les règles suivantes :

1. Pour les sessions en envoi individuel, le AUTH_DATA d'application est copié du bond précédent.
2. Pour les messages en diffusion groupée, le AUTH_DATA d'application est soit le premier AUTH_DATA d'application dans le message, soit choisi par le PDP.

6. Règles de traitement de message

6.1 Génération de message (hôte RSVP)

Un message RSVP est créé comme spécifié dans la [RFC2205] avec les modifications suivantes.

1. Le message RSVP PEUT contenir plusieurs éléments de politique AUTH_DATA.
2. L'élément de politique d'authentification (AUTH_DATA) est créé et le champ IdentityType est réglé de façon à indiquer le type d'identité dans l'élément de politique.
   - DN est inséré comme attribut LOCALISATEUR_DE_POLITIQUE.
   - Des accréditifs tels qu'un ticket Kerberos ou un certificat numérique sont insérés comme attribut ACCREDITIF.

3. L'objet POLICY_DATA (qui contient l'élément de politique AUTH_DATA) est inséré dans le message RSVP à l'endroit approprié. Si l'objet INTEGRITY n'est pas calculé pour le message RSVP, un objet INTEGRITY DEVRAIT alors être calculé pour cet objet POLICY_DATA, comme décrit dans la [RFC2750], et DEVRAIT être inséré comme option de données de politique.

6.2 Réception de message (au routeur)

Le message RSVP est traité comme spécifié dans la [RFC2205] avec les modifications suivantes.

1. Si le routeur n'a pas de capacité politique, il DEVRAIT alors envoyer le message RSVP au PDP et attendre sa réponse. Si le router n'a pas de capacité de politique, il ignore alors les objets de données de politique et continue de traiter le message RSVP.
2. Rejette le message si la réponse du PDP est négative.
3. Continue le traitement du message RSVP.

6.3 Authentification (routeur/PDP)

1. Restitution de l'élément de politique AUTH_DATA. Vérifier le champ Type de PE et retourner une erreur si le type d'identité n'est pas accepté.
2. Vérifier l'accréditif de l'usager.
   - authentification simple : par exemple, obtenir l'identifiant d'usager et le valider, ou obtenir le nom de l'exécutable et le valider.
   - Kerberos : envoyer le ticket Kerberos au KDC pour obtenir la clé de session. L'utilisation de la clé de session authentifie l'usager.
   - clé publique : elle valide le certificat qui a été produit par une autorité de certificat (CA) de confiance et authentifie l'usager ou application en vérifiant la signature numérique.

7. Signalisation d'erreur

Si le PDP échoue à vérifier l'élément de politique AUTH_DATA, il DOIT alors retourner un échec de contrôle de politique (code d'erreur = 02) au PEP. Les valeurs d'erreur sont décrites dans la [RFC2205] et la [RFC2750]. Le PDP DEVRAIT aussi fournir un objet de données de politique contenant un élément de politique AUTH_DATA avec un A-Type = CODE_D'ERREUR_DE_POLITIQUE contenant plus de détails sur l'échec de contrôle de politique (voir au paragraphe 3.3.4). Le PEP va inclure cet objet de données de politique dans le message d'erreur RSVP sortant.

8. Considérations relatives à l'IANA

Suivant la politique exposée dans la [RFC2434], les éléments de politique RSVP standard (valeurs de P-type) sont allouées par action de consensus de l'IETF comme décrit dans la [RFC2750].

Le P-Type AUTH_USER reçoit la valeur 2. Le P-Type AUTH_APP reçoit la valeur 3.

Suivant les politiques exposées dans la [RFC2434], les types d'attribut d'authentification (A-Type) dans la gamme 0-127 sont alloués par action de consensus de l'IETF, les valeurs de A-Type entre 128-255 sont réservées pour usage privé et ne sont pas allouées par l'IANA.

Le A-Type LOCALISATEUR_DE_POLITIQUE reçoit la valeur 1. Le A-Type ACCREDITIF reçoit la valeur 2. Le A-Type SIGNATURE_NUMERIQUE reçoit la valeur 3. Le A-Type OBJET_D'ERREUR_DE_POLITIQUE reçoit la valeur 4.

Suivant les politiques exposées dans la [RFC2434], les valeurs de sous-type de LOCALISATEUR_DE_POLITIQUE dans la gamme de 0 à 127 sont allouées par action de consensus de l'IETF, les valeurs de sous-type LOCALISATEUR_DE_POLITIQUE entre 128 et 255 sont réservées pour usage privé et ne sont pas allouées par l'IANA.

Le sous-type LOCALISATEUR_DE_POLITIQUE ASCII_DN reçoit la valeur 1, le sous-type UNICODE_DN reçoit la valeur 2, le sous-type ASCII_DN_ENCRYPT reçoit la valeur 3 et le sous-type UNICODE_DN_ENCRYPT reçoit la valeur 4.

Suivant les politiques exposées dans la [RFC2434],les valeurs de sous-type ACCREDITIF dans la gamme de 0 à 127 sont allouées par action de consensus de l'IETF, les valeurs de sous-type ACCREDITIF entre 128 et 255 sont réservées pour usage privé et ne sont pas allouées par l'IANA.

Le sous-type ACCREDITIF ASCII_ID reçoit la valeur 1, le sous-type UNICODE_ID reçoit la valeur 2, le sous-type KERBEROS_TKT reçoit la valeur 3, le sous-type X509_V3_CERT reçoit la valeur 4, le sous-type PGP_CERT reçoit la valeur 5.

Suivant les politiques exposées dans la [RFC2434], les valeurs d'erreur dans la gamme de 0 à 32767 sont allouées par action de consensus de l'IETF, les valeurs d'erreur entre 32 768 et 65 535 sont réservées pour utilisation privée et ne sont pas allouées par l'IANA.

La valeur d'erreur ERROR_NO_MORE_INFO reçoit la valeur 1, UNSUPPORTED_CREDENTIAL_TYPE reçoit la valeur 2, INSUFFICIENT_PRIVILEGES reçoit la valeur 3, EXPIRED_CREDENTIAL reçoit la valeur 4, et IDENTITY_CHANGED reçoit la valeur 5.

9. Considérations pour la sécurité

L'objet de ce mémoire est de décrire un mécanisme pour authentifier les demandes RSVP sur la base de l'identité d'utilisateur d'une manière sûre. L'objet RSVP INTEGRITY est utilisé pour protéger l'objet de politique contenant les informations d'identité d'utilisateur contre les attaques (en répétition). La combinaison de l'élément de politique AUTH_DATA et de l'objet INTEGRITY résulte en un contrôle d'accès sécurisé qui met en application une authentification fondée à la fois sur l'identité de l'utilisateur et sur l'identité du nœud d'origine.

L'authentification simple ne contient pas d'accréditif qui puisse être authentifié en toute sécurité et est par nature moins sûr.

Le mécanisme d'authentification Kerberos est raisonnablement sûr.

L'authentification d'utilisateur qui utilise un certificat de clé publique est connu pour fournir la plus forte sécurité.

10. Remerciements

Nous tenons à remercier Andrew Smith, Bob Lindell et beaucoup d'autres de leurs précieux commentaires sur ce mémoire.

11. Références

[ASCII] Coded Character Set -- 7-Bit American Standard Code for Information Interchange, ANSI X3.4- 1986.

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

[RFC2750] S. Herzog, "Extensions à RSVP pour le contrôle de politique", janvier 2000. *(P.S.)*

[RFC2753] R. Yavatkar, D. Pendarakis, R. Guerin, "Cadre pour le contrôle d'admission fondé sur la politique", janvier 2000. *(Info.)*

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir 4120)*

[RFC1704] N. Haller et R. Atkinson, "Authentification sur l'Internet", octobre 1994. *(Information)*

[RFC1779] S. Kille, "Représentation de chaîne des noms distinctifs", mars 1995. *(Obsolète, voir* RFC2253, RFC3494*) (Historique)*

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495) *(P.S.)*

[RFC2209] R. Braden, L. Zhang, "Protocole de réservation de ressource (RSVP) -- version 1 : règles de traitement de message", septembre 1997. *(Information)*

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

[RFC2459] R. Housley, W. Ford, W. Polk et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de CRL pour l'Internet", janvier 1999. *(Obsolète, voir la RFC 3280) (P.S.)*

[RFC2751] S. Herzog, "Élément de politique de priorité par préemption signalé", janvier 2000. (*Obsolète, voir* RFC3181) *(P.S.)*

[UNICODE] The Unicode Consortium, "The Unicode Standard, Version 2.0", Addison-Wesley, Reading, MA, 1996.

[X.509-ITU] UIT-T (ex CCITT) "Technologies de l'Information - Interconnexion des systèmes ouverts – L'Annuaire : Cadre d'authentification", Recommandation X.509, norme ISO/CEI 9594-8.

12. Adresse des auteurs

Satyendra Yadav
Intel, JF3-206
2111 NE 25th Avenue
Hillsboro, OR 97124
mél : Satyendra.Yadav@intel.com

Raj Yavatkar
Intel, JF3-206
2111 NE 25th Avenue
Hillsboro, OR 97124
mél : Raj.Yavatkar@intel.com

Ramesh Pabbati
Microsoft
1 Microsoft Way
Redmond, WA 98054
mél : rameshpa@microsoft.com

Peter Ford
Microsoft
1 Microsoft Way
Redmond, WA 98054
mél : peterf@microsoft.com

Tim Moore
Microsoft
1 Microsoft Way
Redmond, WA 98054
mél : timmoore@microsoft.com

Shai Herzog
PolicyConsulting.Com
200 Clove Rd.
New Rochelle, NY 10801
mél : herzog@policyconsulting.com

Rodney Hess
Intel, BD1
28 Crosby Drive
Bedford, MA 01730
mél : rodney.hess@intel.com

13. Déclaration de droits de reproduction

Remerciement

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