Groupe de travail Réseau
Request for Comments : 3520
Catégorie : En cours de normamisation
Traduction Claude Brière de L'Isle

L-N. Hamer & B. Gage, Nortel Networks
B. Kosinski, Invidi Technologies
H. Shieh, AT&T Wireless
avril 2003

Élément de politique Autorisation de session

Résumé
Le présent document décrit la représentation d'un élément de politique d'autorisation de session pour la prise en charge, l'autorisation et le contrôle d'admission session par session fondé sur la politique. Le but de l'autorisation de session est de permettre l'échange d'informations entre des éléments de réseau afin d'autoriser l'utilisation de ressources pour un service et de coordonner les actions entre les plans de signalisation et de transport. Le présent document décrit comment un processus sur un système autorise la réservation de ressources par un hôte et fournit ensuite à cet hôte un élément de politique d'autorisation de session qui peut être inséré dans un protocole de réservation de ressource (par exemple, le message PATH du protocole de réservation de ressource (RSVP, *Resource ReSerVation Protocol*)) pour faciliter une réservation appropriée et sûre de ces ressources au sein du réseau. On décrit le codage des informations d'autorisation de session comme un élément de politique se conformant au format d'un objet Données de politique [RFC2750] et on fournit le détail du fonctionnement, des règles de traitement et des scénarios d'erreur.

Table des Matières

1. Conventions utilisées dans le document

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

2. Introduction

RSVP [RFC2205] est un exemple de protocole de réservation de ressources qui est utilisé par un hôte pour demander des services spécifiques au réseau pour des courants ou flux de données d'application particuliers. Les demandes RSVP vont généralement résulter en une réservation de ressources dans chaque routeur le long du chemin des données. RSVP permet aux usagers d'obtenir un accès préférentiel aux ressources du réseau, sous le contrôle d'un mécanisme de contrôle d'admission. Un tel contrôle d'admission est souvent fondé sur l'identité de l'usager ou de l'application [RFC3182], cependant, il est aussi valable de fournir une capacité de contrôle d'admission session par session.

Afin de permettre le contrôle d'admission session par session, il est nécessaire de fournir un mécanisme pour s'assurer que l'utilisation de ressources par un hôte a été correctement autorisée avant de permettre la réservation de ces ressources. Pour satisfaire cette exigence, il doit y avoir des informations dans le message de réservation de ressource qui peuvent être utilisées pour vérifier la validité de la demande de réservation. Cela peut être fait en fournissant à l'hôte un élément de politique d'autorisation de session qui est inséré dans le message de réservation de ressource et vérifié par le réseau.

Le présent document décrit l'élément de politique d'autorisation de session (AUTH_SESSION) utilisé pour convoyer les informations sur les ressources dont l'utilisation est autorisée par une session. L'hôte doit obtenir un élément AUTH_SESSION d'une entité d'autorisation via un protocole de signalisation de session tel que SIP [RFC3261]. L'hôte insère alors l'élément AUTH_SESSION dans le message de réservation de ressource pour permettre la vérification de la demande de ressources du réseau ; dans le cas de RSVP, cet élément DOIT être encapsulé dans l'objet Données de politique [RFC2750] d'un message PATH RSVP. Les éléments de réseau vérifient la demande puis traitent le message de réservation de ressource sur la base de la politique d'admission.

La [RFC3521] décrit un cadre dans lequel un élément de politique d'autorisation de session peut être utilisé pour contenir des informations pertinentes pour la décision du réseau de satisfaire une demande de réservation.

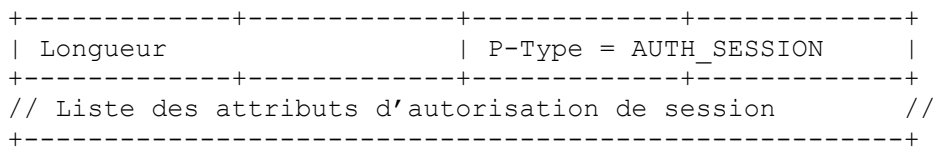
3. Élément de politique pour autorisation de session

3.1 Format d'objet Données de politique

L'élément de politique d'autorisation de session se conforme au format d'un objet POLICY_DATA qui contient les informations de politique et est porté par des protocoles d'admission fondés sur la politique tels que RSVP. Une description détaillée de l'objet POLICY_DATA se trouve dans "Extensions RSVP pour le contrôle de politique" [RFC2750].

3.2 Élément de politique Autorisation de session

Dans ce paragraphe, on décrit un élément de politique (PE, *policy element*) appelé autorisation de session (AUTH_SESSION). L'élément de politique AUTH_SESSION contient une liste de champs qui décrivent la session, ainsi que les autres attributs.



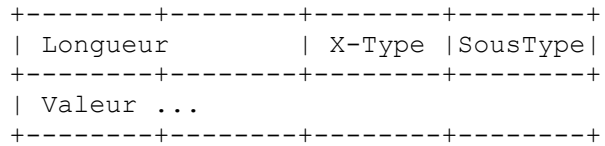
Longueur : 16 bits
La longueur de l'élément de politique (incluant Longueur et P-Type) est en nombre d'octets (DOIT être un multiple de 4) et indique la fin du bloc d'informations d'autorisation de session.

P-Type : 16 bits (type d'autorisation de session) AUTH_SESSION = 0x04. c'est le type d'élément de politique (P-type) de cet élément. L'Autorité d'allocation des numéros de l'Internet (IANA) agit comme registraire des types d'élément de politique comme décrit dans la [RFC2750].

Liste des attributs d'autorisation de session : longueur variable.
La liste des attributs d'autorisation de session est une collection d'objets qui décrivent la session et fournissent d'autres informations nécessaires pour vérifier la demande de réservation de ressources. Un ensemble initial d'objets valides est décrit au paragraphe 3.3.

3.3 Attributs d'autorisation de session

Un attribut d'autorisation de session peut contenir diverses informations et a un type d'attribut et un sous type. L'attribut lui-même DOIT être un multiple de 4 octets, et tout attribut qui n'est pas un multiple de 4 octets DOIT être bourré de zéros jusqu'à une frontière de 4 octets. Tous les octets de bourrage DOIVENT avoir une valeur de zéro.



Longueur : 16 bits
Le champ Longueur fait deux octets et indique la longueur réelle de l'attribut (incluant les champs Longueur, X-Type et SousType) en nombre d'octets. La longueur N'INCLUT PAS d'octets de bourrage dans le champ de valeur pour faire de la longueur de l'attribut un multiple de 4 octets.

X-Type : 8 bits
Le champ Type d'attribut d'autorisation de session (X-Type) fait un octet. IANA agit comme registre pour les X-Types comme décrit à la Section 7, Considérations relatives à l'IANA. Initialement, le registre contient les X-Types suivants :

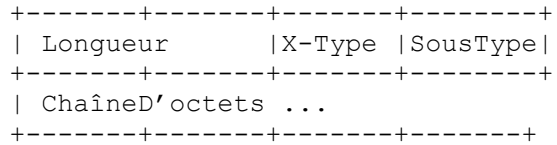
1	AUTH_ENT_ID	identifiant univoque de l'entité qui autorise la session.
2	SESSION_ID	identifiant univoque de cette session.
3	SOURCE_ADDR	spécification de l'adresse de l'origine de la session.
4	DEST_ADDR	spécification de l'adresse du point d'extrémité de la session.
5	START_TIME	heure de début de la session.
6	END_TIME	heure de fin de la session.
7	RESOURCES	ressources que l'usager est autorisé à demander.
8	AUTHENTICATION_DATA	données d'authentification de l'élément de politique d'autorisation de session.

SousType : 8 bits
Le sous-type d'attribut d'autorisation de session est long d'un octet. La valeur du SousType dépend du X-Type.

Valeur : longueur variable. Informations spécifiques de l'attribut.

3.3.1 Identifiant de l'entité d'autorisation

AUTH_ENT_ID est utilisé pour identifier l'entité qui a autorisé la demande de service initiale et généré l'élément de politique d'autorisation de session. AUTH_ENT_ID peut être représenté dans divers formats, et le sous type est utilisé pour définir le format de l'identifiant. Le format de AUTH_ENT_ID est le suivant :



Longueur : Longueur de l'attribut, qui DOIT être > 4.

X-Type : AUTH_ENT_ID

SousTypeLes sous-types suivants sont définis pour AUTH_ENT_ID. L'IANA agit comme registre pour les sous-types de

AUTH_ENT_ID comme décrit à la Section 7. Initialement, le registre contient les sous-types suivants de AUTH_ENT_ID :

1	IPV4_ADDRESS	adresse IPv4 représentée en 32 bits
2	IPV6_ADDRESS	adresse IPv6 représentée en 128 bits
3	FQDN	nom de domaine pleinement qualifié, défini dans la RFC1034 comme une chaîne ASCII.
4	ASCII_DN	nom distinctif X.500, défini dans la RFC2253 comme une chaîne ASCII.
5	UNICODE_DN	nom distinctif X.500, défini dans la RFC2253 comme une chaîne UTF-8.
6	URI	identifiant de ressource universel, comme défini dans la RFC2396.
7	KRB_PRINCIPAL	nom principal Kerberos pleinement qualifié représenté par la chaîne ASCII d'un principal suivi par @ nom de domaine comme défini dans la RFC1510 (par exemple, principalX@domaineY).
8	X509_V3_CERT	nom distinctif du sujet du certificat, défini dans la RFC2253 comme une chaîne UTF-8.
9	PGP_CERT	certificat numérique PGP de l'entité d'autorisation, comme défini dans la RFC2440.

ChaîneD'Octets : Contient l'identifiant de l'entité qui autorise.

3.3.2 Identifiant de session

SESSION_ID est un identifiant univoque utilisé par l'entité d'autorisation pour identifier la demande. Il peut être utilisé pour divers objets, incluant la détection de réponse, ou pour corréler cette demande et une entrée de décision de politique faite par l'entité d'autorisation. Par exemple, SESSION_ID peut se fonder sur un simple numéro de séquence ou sur un horodatage NTP standard.

```
+-------+-------+-------+--------+
| Longueur      |X-Type |SousType|
+-------+-------+-------+--------+
| ChaîneD'Octets ...
+-------+-------+-------+-------+
```

Longueur : longueur de l'attribut, qui DOIT être > 4.

X-Type : SESSION_ID

SousType
Aucun sous type n'est actuellement défini pour SESSION_ID ; ce champ DOIT être réglé à zéro. L'entité d'autorisation est la seule entité réseau qui ait besoin d'interpréter le contenu de SESSION_ID, donc le contenu et le format dépendent de la mise en œuvre.

ChaîneD'Octets : Contient l'identifiant de session.

3.3.3 Adresse de source

SOURCE_ADDR est utilisé pour identifier la spécification de l'adresse de source de la session autorisée. Ce X-Type peut être utile dans certains scénarios pour s'assurer que la demande de ressource a bien été autorisée pour cette adresse et /ou accès de source particuliers.

```
+-------+-------+-------+--------+
| Longueur      |X-Type |SousType|
+-------+-------+-------+--------+
| ChaîneD'Octets ...
+-------+-------+-------+-------+
```

Longueur : Longueur de l'attribut, qui DOIT être > 4.
X-Type : SOURCE_ADDR

SousType
Les sous-types suivants sont définis pour SOURCE_ADDR. L'IANA tient le registre des sous-types SOURCE_ADDR comme décrit à la Section 7. Initialement, le registre contient les sous-types suivants pour SOURCE_ADDR :

1	IPV4_ADDRESS	adresse IPv4 représentée sur 32 bits
2	IPV6_ADDRESS	adresse IPv6 représentée sur 128 bits
3	UDP_PORT_LIST	liste des spécifications d'accès, représentée par 16 bits par entrée de la liste.
4	TCP_PORT_LIST	liste des accès TCP, représentée par 16 bits par entrée de la liste.

ChaîneD'Octets : ChaîneD'Octets contient les informations d'adresse de source.

Dans les scénarios où une adresse de source est requise (voir la Section 5) au moins un des sous-types 1 à 2 (inclus) DOIT être inclus dans chaque élément de politique de données d'autorisation de session. Plusieurs attributs SOURCE_ADDR PEUVENT être inclus si plusieurs adresses ont été autorisées. Le champ Adresse de source du datagramme de réservation de ressource (par exemple, RSVP PATH) DOIT correspondre à un des attributs SOURCE_ADDR contenu dans cet élément de politique de données d'autorisation de session.

Au plus, une instance du sous-type 3 PEUT être incluse dans chaque élément de politique de données d'autorisation de session. Au plus, une instance du sous-type 4 PEUT être incluse dans chaque élément de politique de données d'autorisation de session. L'inclusion d'un attribut de sous-type 3 n'empêche pas l'inclusion d'un attribut de sous-type 4 (c'est-à-dire que des accès UDP et TCP peuvent tous deux être autorisés).

Si aucun attribut PORT n'est spécifié, alors tous les accès sont considérés comme valides ; autrement, seul les accès spécifiés sont autorisés.

Chaque liste d'adresses et accès de source doit être incluse dans un attribut SOURCE_ADDR séparé.

3.3.4 Adresse de destination

DEST_ADDR est utilisé pour identifier l'adresse de destination de la session autorisée. Ce X-Type peut être utile dans certains scénarios pour s'assurer que la demande de ressources a été autorisée pour cette adresse ou accès de destination particulier.

```
+-------+-------+-------+--------+
| Longueur      |X-Type |SousType|
+-------+-------+-------+--------+
| ChaîneD'Octets ...
+-------+-------+-------+-------+
```

Longueur : Longueur de l'attribut, qui DOIT être > 4.

X-Type : DEST_ADDR

SousType
Les sous-types suivants sont définis pour DEST_ADDR. L'IANA tient un registre des sous-types DEST_ADDR comme décrit à la Section 7. Initialement, le registre contient les sous-types suivants pour DEST_ADDR :

1 IPV4_ADDRESS adresse IPv4 représentée sur 32 bits
2 IPV6_ADDRESS adresse IPv6 représentée sur 128 bits
3 UDP_PORT_LIST liste des spécifications d'accès UDP, représentées par 16 bits par entrée de liste.
4 TCP_PORT_LIST liste des spécifications d'accès TCP, représentées par 16 bits par entrée de liste.

ChaîneD'Octets : contient l'adresse de destination.

Dans les scénarios où une adresse de destination est exigée (voir la Section 5) au moins un des sous-types 1 à 2 (inclus) DOIT être inclus dans chaque élément de politique de données d'autorisation de session. Plusieurs attributs DEST_ADDR PEUVENT être inclus si plusieurs adresses ont été autorisées. Le champ Adresse de destination du datagramme de réservation de ressource (par exemple, RSVP PATH) DOIT correspondre à un des attributs DEST_ADDR contenu dans cet élément de politique de données d'autorisation de session.

Au plus, une instance du sous-type 3 PEUT être incluse dans chaque élément de politique de données d'autorisation de session. Au plus, une instance du sous-type 4 PEUT être incluse dans chaque élément de politique de données d'autorisation de session. L'inclusion d'un attribut du sous-type 3 n'empêche pas l'inclusion d'un attribut de sous-type 4 (c'est-à-dire, des accès UDP et TCP peuvent tous deux être autorisés).

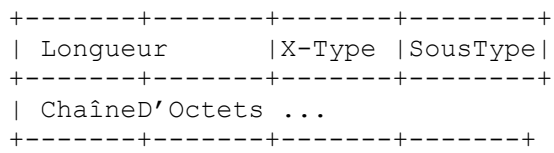
Si aucun attribut PORT n'est spécifié, alors tous les accès sont considérés comme valides ; autrement, seul les accès spécifiés sont autorisés.

Chaque liste d'adresse et accès de destination doit être incluse dans un attribut DEST_ADDR séparé.

3.3.5 Heure de début

START_TIME est utilisé pour identifier le début de la session autorisée et peut être utilisé pour empêcher des attaques en

répétition. Si l'élément de politique AUTH_SESSION est présenté dans une demande de ressource, le réseau DEVRAIT rejeter la demande si elle n'est pas reçue dans les quelques secondes de l'heure de début spécifiée.



Longueur : Longueur de l'attribut, qui DOIT être > 4.

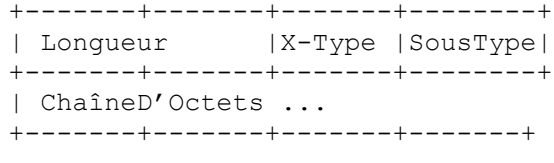
X-Type : START_TIME

SousType
Les sous-types suivants sont définis pour START_TIME. L'IANA agit comme registre pour les sous-types START_TIME comme décrit à la Section 7. Initialement, le registre contient les sous-types suivants pour START_TIME :
1 NTP_TIMESTAMP format d'horodatage NTP comme défini dans la RFC1305.

ChaîneD'Octets : contient l'heure de début.

3.3.6 Heure de fin

END_TIME est utilisé pour identifier l'heure de fin de la session autorisée et peut être utilisé pour limiter la durée pendant laquelle l'utilisation des ressources est autorisée (par exemple, dans un scénario de session prépayée).



Longueur : Longueur de l'attribut, qui DOIT être > 4.

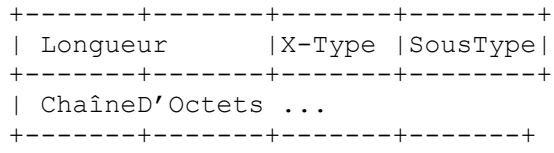
X-Type : END_TIME

SousType
Les sous-types suivants sont définis pour END_TIME. L' IANA tient un registre pour les sous-types END_TIME comme décrit à la Section 7. Initialement, le registre contient les sous-types suivants pour END_TIME :
1 NTP_TIMESTAMP Format d'horodatage NTP comme défini dans la RFC1305.

ChaîneD'Octets : contient l'heure de fin.

3.3.7 Ressources autorisées

RESOURCES est utilisé pour définir les caractéristiques de la session autorisée. Ce X-Type peut être utile dans certains scénarios pour spécifier les ressources spécifiques autorisées pour s'assurer que la demande respecte les spécifications autorisées.



Longueur : Longueur de l'attribut, qui DOIT être > 4.
X-Type : RESOURCES
SousType
On définit les sous-types suivants pour RESOURCES. L'IANA tient un registre des sous-types RESOURCES, comme décrit à la Section 7. Initialement, le registre contient les sous-types suivants pour RESOURCES :
1 BANDWIDTH bande passante maximum (kbit/s) autorisée.
2 FLOW_SPEC spécification du flux comme défini dans la RFC2205.
3 SDP descripteur de support SDP comme défini dans la RFC2327.

4 DSCP codets de service différenciés comme défini dans la RFC2474.

ChaîneD'Octets : contient la spécification de la ressource.

Dans les scénarios où une spécification de ressource est exigée (voir la Section 5) au moins un des sous-types 1 à 4 (inclus) DOIT être inclus dans tout élément de politique de données d'autorisation de session. Plusieurs attributs RESOURCE PEUVENT être inclus si plusieurs types de ressources ont été autorisés (par exemple, DSCP et BANDWIDTH).

3.3.8 Données d'authentification

L'attribut AUTHENTICATION_DATA contient les données d'authentification de l'élément de politique AUTH_SESSION et signe toutes les données dans l'élément de politique jusqu'à AUTHENTICATION_DATA. Si l'attribut AUTHENTICATION_DATA a été inclus dans l'élément de politique AUTH_SESSION, il DOIT être le dernier attribut de la liste. L'algorithme utilisé pour calculer les données d'authentification dépend du champ SousType AUTH_ENT_ID. Voir la Section 4 ci-dessous.

Un résumé du format de l'attribut AUTHENTICATION_DATA est décrit ci-dessous.

```
+-------+-------+-------+--------+
| Longueur      |X-Type |SousType|
+-------+-------+-------+--------+
| ChaîneD'Octets ...
+-------+-------+-------+--------+
```

Longueur : Longueur de l'attribut, qui DOIT être > 4.
X-Type : AUTHENTICATION_DATA
SousType : Aucun sous-type n'est actuellement défini pour AUTHENTICATION_DATA. Ce champ DOIT être à 0.
ChaîneD'Octets : contient les données d'authentification de AUTH_SESSION.

4. Intégrité de l'élément de politique AUTH_SESSION

Cette section décrit comment s'assurer que l'intégrité de l'élément de politique est préservée.

4.1 Clés symétriques partagées

Dans les environnements de clé symétrique partagée, AUTH_ENT_ID DOIT être des sous-types : IPV4_ADDRESS, IPV6_ADDRESS, FQDN, ASCII_DN, UNICODE_DN ou URI. Un exemple d'élément de politique AUTH_SESSION est montrée ci-dessous.

```
+-------------+-------------+-------------+-------------+
| Longueur                  | P-type = AUTH_SESSION       |
+-------------+-------------+-------------+-------------+
| Longueur                  |SESSION_ID   |     zéro    |
+-------------+-------------+-------------+-------------+
| ChaîneD'Octets (identifiant de session) ...
+-------------+-------------+-------------+-------------+
| Longueur                  | AUTH_ENT_ID | IPV4_ADDRESS |
+-------------+-------------+-------------+-------------+
| ChaîneD'Octets (Identifiant de l'entité qui autorise) ...
+-------------+-------------+-------------+-------------+
| Longueur                  |AUTH DATA.   |     zéro    |
+-------------+-------------+-------------+-------------+
|                        KEY_ID                         |
+-------------+-------------+-------------+-------------+
| ChaîneD'Octets (données d'authentification) ...
+-------------+-------------+-------------+-------------+
```

4.1.1 Réglage pour un fonctionnement avec clés symétriques partagées

On suppose que l'entité qui autorise et le routeur /PDP réseau sont tous deux provisionnés avec des clés symétriques

partagées et des politiques qui précisent quel algorithme utiliser pour calculer les données d'authentification ainsi que la longueur attendue des données d'authentification pour cet algorithme.

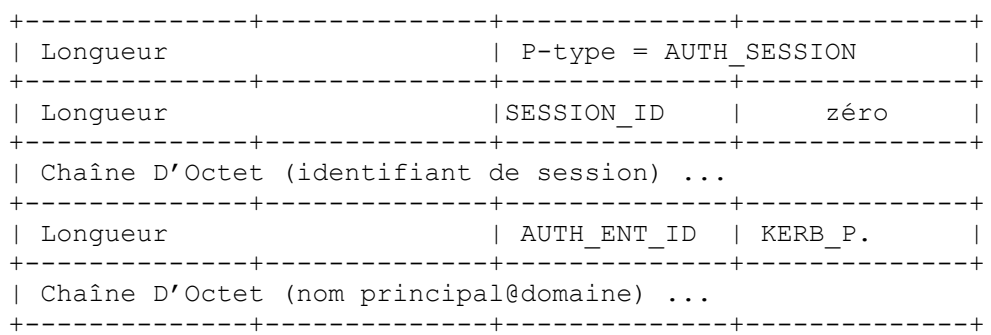
La gestion des clés sort du domaine d'application du présent document, mais les mises en œuvre de AUTH_SESSION DOIVENT au moins fournir la capacité de configuration manuelle des clés et de leurs paramètres en local. La clé utilisée pour produire les données d'authentification est identifiée par le champ AUTH_ENT_ID. Comme plusieurs clés peuvent être configurées pour une valeur particulière de AUTH_ENT_ID, les 32 premiers bits du champ AUTH_DATA DOIVENT être un identifiant de clé à utiliser pour identifier la clé appropriée. Chaque clé doit aussi être configurée avec des paramètres de durée de vie pendant laquelle elle est valide ainsi que le paramètre d'algorithme de chiffrement associé qui spécifie l'algorithme à utiliser avec la clé. Au minimum, toutes les mises en œuvre de AUTH_SESSION DOIVENT prendre en charge l'algorithme de chiffrement HMAC-MD5-128 [RFC2104], [RFC1321] pour calculer les données d'authentification. De nouveaux algorithmes pourront être ajoutés par le processus de normalisation de l'IETF.

Il est de bonne pratique de changer régulièrement les clés. Les clés DOIVENT être configurables de telle façon que leur durée de vie se chevauche pour permettre une transition en douceur entre les clés. Au milieu du chevauchement de la durée de vie entre deux clés, les envoyeurs devraient passer de l'utilisation de la clé actuelle à la prochaine clé de plus longue durée de vie. Pendant ce temps, les receveurs acceptent simplement toute clé identifiée reçue au sein de sa durée de vie configurée et rejettent celles qui ne le sont pas.

4.2 Kerberos

Dans un environnement Kerberos, l'identifiant AUTH_ENT_ID DOIT être du sous-type KRB_PRINCIPAL. Le champ KRB_PRINCIPAL est défini comme le nom de principal Kerberos pleinement qualifié de l'entité d'autorisation. L'authentification Kerberos [RFC1510] utilise un tiers de confiance (le centre de distribution Kerberos (KDC, *Kerberos Distribution Center*)) pour assurer l'authentification de la AUTH_SESSION auprès d'un serveur réseau. On suppose qu'un KDC est présent et que l'hôte et le vérificateur des informations d'authentification (entité d'autorisation et routeur/PDP) mettent tous deux en œuvre l'authentification Kerberos.

Un exemple de l'élément de politique AUTH_DATA Kerberos est montré ci-dessous.



4.2.1 Réglage du fonctionnement avec Kerberos

Une entité d'autorisation est configurée pour construire l'élément de politique AUTH_SESSION qui désigne l'utilisation de la méthode d'authentification Kerberos (KRB_PRINCIPAL) comme défini dans la RFC1510. À réception de la demande de réservation de ressource, le routeur/PDP contacte le KDC local, avec un message KRB_AS_REQ, pour demander des accréditifs pour l'entité d'autorisation (principal@domaine). Dans cette demande, le client (routeur/PDP) envoie (en clair) sa propre identité et l'identité du serveur (l'entité d'autorisation prise dans le champ AUTH_ENT_ID) pour laquelle il demande des accréditifs. Le KDC local répond avec ces accréditifs dans un message KRB_AS_REP, chiffré dans la clé du client. Les accréditifs consistent en 1) un "ticket" pour le serveur et 2) une clé de chiffrement temporaire (souvent appelée "clé de session"). Le routeur/PDP utilise le ticket pour accéder à l'entité d'autorisation avec un message KRB_AP_REQ. La clé de session (maintenant partagée par le routeur/PDP et l'entité d'autorisation) est utilisée pour authentifier le routeur/PDP, et est utilisée pour authentifier l'entité d'autorisation. La clé de session est une clé de chiffrement et est aussi utilisée pour chiffrer la suite de la communication entre les deux parties. L'entité d'autorisation répond en envoyant un message enchaîné d'une KRB_AP_REP et d'un KRB_SAFE. La KRB_AP_REP est utilisée pour authentifier l'entité d'autorisation. Le message KRB_SAFE contient les données d'authentification dans le champ safe-body. Les données d'authentification doivent être un hachage MD5 de 16 octets ou un hachage SHA-1 de 20 octets de toutes les données dans l'élément de politique AUTH_SESSION jusqu'au AUTHENTICATION_DATA (noter que lors de l'utilisation de Kerberos, l'élément de politique AUTH_SESSION ne devrait pas inclure AUTHENTICATION_DATA car celui-ci est envoyé dans le

message KRB_SAFE). Le routeur/PDP calcule de façon indépendante le hachage et le compare à celui reçu dans le champ user-data du KRB-SAFE-BODY [RFC1510].

Au minimum, toutes les mises en œuvre de AUTH_SESSION qui utilisent Kerberos DOIVENT prendre en charge le type de chiffrement des-cbc-md5 de Kerberos [RFC1510] (pour les données chiffrées dans les tickets et les messages Kerberos) et le type de somme de contrôle Kerberos rsa-md5-des [RFC1510] (pour la somme de contrôle KRB_SAFE). De nouveaux algorithmes pourront être ajoutés par le processus de normalisation de l'IETF. Le codage Triple-DES est pris en charge dans de nombreuses mises en œuvre de Kerberos (bien que non spécifié dans la [RFC1510]) et DEVRAIT être utilisé plutôt que le seul DES.

Pour les cas où l'entité d'autorisation est dans un domaine différent (c'est-à-dire, un domaine administratif, une frontière organisationnelle) le routeur/PDP doit aller cherche un ticket distributeur de tickets (TGT, *Ticket Granting Ticket*) trans-domaine auprès de son KDC local. Ce TGT peut être utilisé pour aller chercher les tickets d'entité d'autorisation auprès du KDC dans le domaine distant. Noter que pour des considérations de performances, les tickets sont normalement mis en antémémoire pendant de longues durées.

4.3 Clé publique

Dans un environnement de clé publique, AUTH_ENT_ID DOIT être des sous-types : X509_V3_CERT ou PGP_CERT. Les données d'authentification sont utilisées pour authentifier l'entité d'autorisation. Un exemple de l'élément de politique AUTH_SESSION de clé publique est montré ci-dessous.

```
+--------------+--------------+--------------+--------------+
| Longueur                    | P-type = AUTH_SESSION       |
+--------------+--------------+--------------+--------------+
| Longueur                    |SESSION_ID    |     zéro     |
+--------------+--------------+--------------+--------------+
| ChaîneD'Octets (identifiant de session) ...
+--------------+--------------+--------------+--------------+
| Longueur                    | AUTH_ENT_ID  |   PGP_CERT   |
+--------------+--------------+--------------+--------------+
| ChaîneD'Octets (Certificat num. de l'entité d'autor.) ...
+--------------+--------------+--------------+--------------+
| Longueur                    |AUTH DATA.    |     zéro     |
+--------------+--------------+--------------+--------------+
| ChaîneD'Octets (données d'authentification) ...
+--------------+--------------+--------------+--------------+
```

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

L'entité d'autorisation utilise sa clé privée pour générer les AUTHENTICATION_DATA. Les authentificateurs (routeur, PDP) utilisent la clé publique de l'entité d'autorisation (mémorisée dans le certificat numérique) pour vérifier et authentifier l'élément de politique.

4.3.1.1 Certificats numériques X.509 v3

Lorsque le AUTH_ENT_ID est du type X509_V3_CERT, AUTHENTICATION_DATA DOIT être généré en suivant ces étapes :

- Un Signed-data est construit comme défini dans la section 5 de la syntaxe de message cryptographique [RFC3369]. Un résumé est calculé sur le contenu (comme spécifié au paragraphe 6.1) avec un algorithme de résumé de message spécifique du signataire. Le champ Certificates contient la chaîne des certificats numériques X.509 v3 de l'entité d'autorisation. La liste de révocation de certificats est définie dans le champ crls. Le résultat du résumé est signé numériquement suivant la Section 8 de la RFC3447, en utilisant la clé privée du signataire.

Lorsque AUTH_ENT_ID est du type X509_V3_CERT, la vérification DOIT être faite selon les étapes suivantes :
- analyser le certificat X.509 v3 pour extraire le nom distinctif du producteur du certificat.
- la validation du chemin de certification est effectuée comme défini dans la section 6 de la RFC3280.
- analyser la liste de révocation de certificats pour vérifier que le certificat reçu n'y figure pas.
- Une fois le certificat X.509 v3 validé, la clé publique de l'entité d'autorisation peut être extraite du certificat.
- Extraire l'algorithme de résumé et la longueur des données résumées en analysant les données de données signées.
- Le receveur calcule de façon indépendante le résumé de message. Celui-ci et la clé publique du signataire sont utilisés pour vérifier la valeur de la signature.

Cette vérification assure l'intégrité, la non répudiation et l'origine des données.

4.3.1.2 Certificats numériques PGP

Lorsque AUTH_ENT_ID est du type PGP_CERT, AUTHENTICATION_DATA DOIT être généré selon les étapes suivantes :
- AUTHENTICATION_DATA contient un paquet Signature comme défini au paragraphe 5.2.3 de la RFC2440. En résumé :
  - Calculer le hachage de toutes les données dans l'élément de politique AUTH_SESSION jusqu'à AUTHENTICATION_DATA.
  - Le résultat du hachage est signé numériquement suivant la section 8 de la RFC3447, en utilisant la clé privée du signataire.

Lorsque AUTH_ENT_ID est du type PGP_CERT, la vérification DOIT être faite suivant ces étapes :
- Valider le certificat.
- Une fois le certificat PGP validé, la clé publique de l'entité d'autorisation peut être extraite du certificat.
- Extraire l'algorithme de hachage et la longueur des données hachées en analysant la paquet de signature du PGP.
- Le receveur calcule indépendamment le résumé du message. Ce résumé de message et la clé publique du signataire sont utilisés pour vérifier la valeur de la signature.

Cette vérification assure l'intégrité, la non répudiation et l'origine des données.

5. Cadre

La [RFC3521] décrit un cadre dans lequel l'élément de politique AUTH_SESSION peut être utilisé pour le transport des informations requises pour autoriser la réservation de ressource pour les flux du support. La [RFC3521] introduit quatre modèles différents :
1- le modèle couplé
2- le modèle associé à un serveur de politique
3- le modèle associe à deux serveurs de politique
4- le modèle non associé.

Les champs qui sont exigés dans un élément de politique AUTH SESSION dépendent du modèle utilisé.

5.1 Modèle couplé

Dans le modèle complet, les seules informations qui DOIVENT être incluses dans l'élément de politique sont celles de SESSION_ID ; il est utilisé par l'entité d'autorisation pour corréler la demande de réservation de ressources avec le support autorisé durant l'établissement de session. Comme l'hôte d'extrémité est supposé n'être pas de confiance, le serveur de politique DEVRAIT prendre des mesures pour s'assurer que l'intégrité du SESSION_ID est préservée dans le transit ; les mécanismes exacts à utiliser et le format du SESSION_ID dépendent de la mise en œuvre.

5.2 Modèle associé à un serveur de politique

Dans ce modèle, le contenu de l'élément de politique AUTH_SESSION DOIVENT inclure :

- Un identifiant de session - SESSION_ID. C'est l'information que l'entité d'autorisation peut utiliser pour corréler la demande de réservation de ressources avec le support autorisé durant l'établissement de session.

- L'identité de l'entité d'autorisation - AUTH_ENT_ID. Cette information est utilisée par le routeur bordure pour déterminer quelle entité d'autorisation (serveur de politique) devrait être utilisée pour solliciter des décisions de politique de ressources.

Dans certains environnements, un routeur bordure peut n'avoir aucun moyen pour déterminer si l'identité se réfère à un serveur de politique légitime au sein de son domaine. Afin de protéger contre la redirection de demandes d'autorisation sur une entité d'autorisation véreuse, le AUTH_SESSION DOIT aussi inclure :
- AUTHENTICATION_DATA. Ces données d'authentification sont calculées sur tous les autres champs de l'élément de politique AUTH_SESSION.

5.3 Modèle associé à deux serveurs de politique

Le contenu de l'élément de politique AUTH_SESSION est identique à celui du modèle associé à un serveur de politique.

5.4 Modèle non associé

Dans ce modèle, le AUTH_SESSION DOIT contenir des informations suffisantes pour permettre au serveur de politique de prendre des décisions de politique de ressources indépendamment de l'entité d'autorisation. L'élément de politique est créé en utilisant les informations de l'entité d'autorisation sur la session. Les informations dans l'élément de politique AUTH_SESSION DOIVENT inclure :
- l'adresse IP ou l'identité de l'appelant (par exemple, FQDN) - SOURCE_ADDR X-TYPE
- l'adresse IP ou l'identité de l'appelé (par exemple, FQDN) - DEST_ADDR X-TYPE
- les caractéristiques de chacun des flux de support autorisés pour cette session - RESOURCES X-TYPE
- la durée de vie de l'autorisation - START_TIME X-TYPE
- l'identité de l'entité d'autorisation pour permettre la validation du jeton dans les schémas de clé symétrique partagée et Kerberos - AUTH_ENT_ID X-TYPE
- les accréditifs de l'entité d'autorisation dans un schéma de clé publique - AUTH_ENT_ID X-TYPE
- les données d'authentification utilisées pour empêcher l'altération de l'élément de politique AUTH_SESSION - AUTHENTICATION_DATA

De plus, l'élément de politique AUTH_SESSION PEUT contenir :
- la durée de vie de chaque flux de support - END_TIME X-TYPE
- le numéro d'accès de l'appelant - SOURCE_ADDR X-TYPE
- le numéro d'accès de l'appelé - DEST_ADDR X-TYPE

Tous les champs de AUTH_SESSION DOIVENT correspondre avec ceux de la demande de ressource. Si un champ ne correspond pas, la demande DEVRAIT être refusée.

6. Règles de traitement du message

6.1 Génération de AUTH_SESSION par l'entité d'autorisation

1. Générer l'élément de politique AUTH_SESSION avec le contenu approprié comme spécifié à la section 5.
2. Si l'authentification est nécessaire, l'élément de politique AUTH_SESSION entier est construit, excluant les champs de longueur, de type et de sous-type du champ AUTH_SESSION. Noter que le message DOIT inclure un START_TIME ou un SESSION_ID (voir la Section 9) pour empêcher les attaques en répétition. Le résultat de l'algorithme d'authentification, plus les informations d'en-tête appropriées, est ajouté à l'élément de politique AUTH_SESSION.

6.2 Génération du message (hôte RSVP)

Un message RSVP est créé comme spécifié dans la [RFC2205] avec les modifications suivantes :
1. Le message RSVP DOIT contenir au plus un élément de politique AUTH_SESSION.
2. L'élément de politique AUTH SESSION reçu de l'entité d'autorisation (paragraphe 3.2) DOIT être copié sans modification dans l'objet POLICY DATA.
3. L'objet POLICY_DATA (qui contient l'élément de politique AUTH_SESSION) est inséré dans le message RSVP à l endroit approprié.

6.3 Réception du message (routeur à capacité RSVP)

Le message RSVP est traité comme spécifié dans la [RFC2205] avec les modifications suivantes :
1. Si le routeur à la capacité de traiter la politique, il DEVRAIT envoyer le message RSVP au PDP et attendre la réponse. Sinon, il ignore les objets de données de politique et continue de traiter le message RSVP.
2. Rejeter le message si la réponse du PDP est négative.
3. Continuer de traiter le message RSVP.

6.4 Autorisation (routeur/PDP)

1. Restituer l'élément de politique AUTH_SESSION. Vérifier le champ Type d'élément de politique et retourner une erreur si le type d'identité n'est pas pris en charge.
2. Vérifier l'intégrité du message.
   - Authentification de clé symétrique partagée : le routeur/PDP réseau utilise le champ AUTH_ENT_ID pour consulter un table chiffré par ce champ. Le tableau devrait identifier l'algorithme d'authentification cryptographique à utiliser ainsi que la longueur attendue des données d'authentification et la clé symétrique partagée pour l'entité d'autorisation. Vérifier que la longueur indiquée des données d'authentification est cohérente avec l'entrée de tableau configurée et valider les données d'authentification.
   - Clé publique : valider la chaîne de certificats par rapport à l'autorité de certificat (CA) de confiance et valider la signature du message en utilisant la clé publique.
   - Ticket Kerberos : si le AUTH_ENT_ID est du sous-type KRB_PRINCIPAL, demander un ticket pour l'entité d'autorisation (principal@domaine) au KDC local. Utiliser le ticket pour accéder à l'entité d'autorisation et obtenir les données d'authentification pour le message.
3. Une fois établies l'identité de l'entité d'autorisation et la validité de la demande de service, le routeur/PDP d'autorisation DOIT alors consulter ses tableaux de politique locale (dont le contenu est une affaire locale) afin de déterminer si la demande spécifique est ou non autorisée. Dans la mesure où ces décisions de contrôle d'accès exigent des informations supplémentaires, les routeurs/PDP DOIVENT s'assurer que les informations supplémentaires sont obtenues en toute sécurité. Un exemple de décision de contrôle d'accès non sûre serait celui où la partie qui autorise s'appuie sur une base de données non sûre (comme le DNS ou un répertoire LDAP public) et autorise avec un certificat ou un FQDN.
4. Vérifier que les ressources demandées n'excèdent pas la QS autorisée.

7. Signalisation d'erreur

Si un PDP échoue à vérifier l'élément de politique AUTH_SESSION, il DOIT alors retourner un échec de commande de politique (code d'erreur = 02) au PEP. Les valeurs d'erreur sont décrite dans la [RFC2205] et la [RFC2750]. Le PDP DEVRAIT aussi fournie un objet de données de politique contenant un élément de politique AUTH_DATA avec A-Type=POLICY_ERROR_CODE contenant plus de détails sur l'échec de commande de politique [RFC3182]. Si RSVP est utilisé, le PEP DOIT inclure cet objet de données de politique dans le message d'erreur RSVP sortant.

8. Considérations relatives à l'IANA

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

P-Type AUTH_SESSION reçoit la valeur 0x04.

Suivant les politiques définies dans la [RFC2434], les types d'attribut d'autorisation de session (X-Type) dans la gamme 0 à 127 sont alloués par une action de consensus de l'IETF ; les valeurs de X-Type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées par l'IANA.
X-Type AUTH_ENT_ID reçoit la valeur 1.
X-Type SESSION_ID reçoit la valeur 2.
X-Type SOURCE_ADDR reçoit la valeur 3.
X-Type DEST_ADDR reçoit la valeur 4.
X-Type START_TIME reçoit la valeur 5.
X-Type END_TIME reçoit la valeur 6.

X-Type RESOURCES reçoit la valeur 7.
X-Type AUTHENTICATION_DATA reçoit la valeur 8.

Suivant les politiques définies dans la [RFC2434], les valeurs de sous type AUTH_ENT_ID dans la gamme de 0 à 127 sont allouées par une action de consensus de l'IETF ; les valeurs de sous type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées pas l'IANA.
le sous -type IPV4_ADDRESS de AUTH_ENT_ID reçoit la valeur 1.
le sous -type IPV6_ADDRESS reçoit la valeur 2.
le sous -type FQDN reçoit la valeur 3.
le sous -type ASCII_DN reçoit la valeur 4.
le sous -type UNICODE_DN reçoit la valeur 5.
le sous -type URI reçoit la valeur 6.
le sous -type KRB_PRINCIPAL reçoit la valeur 7.
le sous -type X509_V3_CERT reçoit la valeur 8.
le sous -type PGP_CERT reçoit la valeur 9.

Suivant les politiques définies dans la [RFC2434], les valeurs de sous-type SOURCE_ADDR dans la gamme de 0 à 127 sont allouées par une action de consensus de l'IETF ; les valeurs de sous-type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées par IANA.
le sous -type IPV4_ADDRESS de SOURCE_ADDR reçoit la valeur 1.
le sous -type IPV6_ADDRESS reçoit la valeur 2.
le sous -type UDP_PORT_LIST reçoit la valeur 3.
le sous -type TCP_PORT_LIST reçoit la valeur 4.

Suivant les politiques définies dans la [RFC2434], les valeurs de sous-type DEST_ADDR dans la gamme de 0 à 127 sont allouées par une action de consensus de l'IETF ; les valeurs de sous-type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées par l'IANA.
le sous -type IPV4_ADDRESS de DEST_ADDR reçoit la valeur 1.
le sous -type IPV6_ADDRESS reçoit la valeur 2.
le sous -type UDP_PORT_LIST reçoit la valeur 3.
le sous -type TCP_PORT_LIST reçoit la valeur 4.

Suivant les politiques définies dans la [RFC2434], les valeurs du sous-type START_TIME dans la gamme de 0 à 127 sont allouées par une action de consensus de l'IETF ; les valeurs de sous-type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées par l'IANA.
le sous-type NTP_TIMESTAMP de START_TIME reçoit la valeur 1.

Suivant les politiques définies dans la [RFC2434], les valeurs de sous-type END_TIME dans la gamme de 0 à 127 sont allouées par une action de consensus de l'IETF ; les valeurs de sous-type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées par l'IANA.
le sous-type NTP_TIMESTAMP de END_TIME reçoit la valeur 1.

Suivant les politiques définies dans la [RFC2434], les valeurs de sous-type RESOURCES dans la gamme de 0 à 127 sont allouées par une action de consensus de l'IETF ; les valeurs de sous-type entre 128 et 255 sont réservées pour utilisation privée et ne sont pas allouées par l'IANA.
le sous-type BANDWIDTH de RESOURCES reçoit la valeur 1.
le sous-type FLOW_SPEC reçoit la valeur 2.
le sous-type SDP reçoit la valeur 3.
le sous-type DSCP reçoit la valeur 4.

9. Considérations sur la sécurité

L'objet du présent est de décrire un mécanisme pour que l'autorisation de session empêche le vol de service.

Les attaques en répétition DOIVENT être empêchées. Dans le modèle non associé, l'élément de politique AUTH_SESSION DOIT inclure un champ START_TIME et les serveurs de politique DOIVENT prendre en charge NTP pour assurer une synchronisation d'horloge appropriée. Manquer à assurer une synchronisation d'horloge appropriée permet les attaques en répétition car les horloges des différentes entités réseau peuvent n'être pas synchronisées. L'heure de début est utilisée pour vérifier que la demande n'a pas été répétée ultérieurement. Dans tous les autres modèles, le SESSION_ID est utilisé par le serveur de politique pour s'assurer que la demande de ressource réussit à se corréler avec les enregistrements d'une session autorisée. Si une AUTH_SESSION est répétée, cela DOIT être détecté par le serveur de

politique (en utilisant des algorithmes internes) et la demande DOIT être rejetée.

Pour s'assurer que l'intégrité de l'élément de politique est préservé dans des environnements qui ne sont pas de confiance, l'attribut AUTHENTICATION_DATA DOIT être inclus.

Dans les environnements où des clés symétriques partagées sont possibles, elles devraient être utilisées afin de garder la taille de l'élément de politique AUTH_SESSION au strict minimum. Ceci est particulièrement vrai dans les environnements sans fils où l'élément de politique AUTH_SESSION est envoyé sur les ondes. L'option d'authentification par clé symétriques partagée DOIT être prise en charge par toutes les mises en œuvre de AUTH_SESSION.

Si les clés symétriques partagées ne sont pas une option valide, le mécanisme d'authentification Kerberos est raisonnablement bien sécurisé et efficace en termes de taille de AUTH_SESSION. AUTH_SESSION a seulement besoin de contenir le nom principal@domaine de l'entité d'autorisation. Ceci est beaucoup plus efficace que l'option d'authentification PKI.

L'option d'authentification PKI donne un haut niveau de sécurité et une bonne adaptabilité, cependant, elle exige la présence d'accréditifs dans l'élément de politique AUTH_SESSION qui ont un impact sur sa taille.

10. Remerciements

Nous tenons à remercier Francois Audet, Don Wade, Hamid Syed, Kwok Ho Chan et beaucopup d'autre de leurs précieux commentaires. Un merci tout particulier à Eric Rescorla qui a fourni de nombreux commentaires et suggestions qui ont amélioré ce document.
De plus, nous aimerions remercier S. Yadav, et les autres, de leurs efforts sur la RFC3182, car le présent document a fait des emprunts à leur travail.

11. Références normatives

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

[X.509] Recommandation UIT-T X.509. "Technologies de l'information - Interconnexion des systèmes ouverts – L'Annuaire : Cadre d'authentification", aussi ISO/CEI 9594-8.

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par* RFC5905)

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir RFC6649)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[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, RFC6780)) *(P.S.)*

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

[RFC2253] M. Wahl, S. Kille et T. Howes, "Protocole léger d'accès à un répertoire (LDAPv3) : Représentation de chaîne UTF-8 des noms distinctifs", décembre 1997.

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

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

[RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (*Obsolète, voir* RFC3986)

[RFC2440] J. Callas, L. Donnerhacke, H. Finney et R. Thayer, "Format de message OpenPGP", novembre 1998. *(Obsolète, voir* RFC4880*)*

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6", décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

[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.)*

[RFC3182] S. Yadav et autres, "Représentation d'identité pour RSVP", octobre 2001. *(P.S.)*

[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*)*

[RFC3369] R. Housley, "Syntaxe de message cryptographique (CMS)", août 2002. (*Obsolète, voir* RFC3852) *(P.S.)*

[RFC3447] J. Jonsson et B. Kaliski, "Normes de cryptographie à clés publiques (PKCS) n° 1 : Spécifications de la cryptographie RSA version 2.1", février 2003.

[RFC3521] L-N. Hamer, B. Gage, H. Shieh, "Cadre de l'établissement de session avec autorisation du support", avril 2003. *(Info.)*

12. Références pour information

[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*)*

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

13. 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.

14. Contributeurs

Matt Broda
Nortel Réseaux
mél : mbroda@nortelréseaus.com

Louis LeVay
Nortel Réseaus
mél : levay@nortelréseaus.com

Dennis Beard
Nortel Réseaus
mél : beardd@nortelréseaus.com

Lawrence Dobranski
Nortel Réseaus
mél : ldobran@nortelréseaus.com

15. Adresses des auteurs

Louis-Nicolas Hamer
Nortel Réseaus
PO Box 3511 Station C
Ottawa, Ontario
Canada K1Y 4H7
téléphone : +1 613.768.3409
mél : nhamer@nortelréseaus.com

Brett Kosinski
Invidi Technologies
Edmonton, Alberta
Canada T5J 3S4
mél : brettk@invidi.com

Bill Gage
Nortel Réseaus
PO Box 3511 Station C
Ottawa, Ontario
Canada K1Y 4H7
téléphone : +1 613.763.4400
mél : gageb@nortelréseaus.com

Hugh Shieh
AT&T Wireless
7277 164th Avenue NE
Redmond, WA
USA 98073-9761
téléphone : +1 425.580.6898
mél : hugh.shieh@attws.com

16. Déclaration complète de droits de reproduction

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