Groupe de travail Réseau
Request for Comments : 4681
RFC mise à jour : 4346
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

S. Santesson, Microsoft
A. Medvinsky, Microsoft
J. Ball, Microsoft

octobre 2006

Extension de transposition d'utilisateur TLS

Résumé
Le présent document spécifie une extension à TLS qui permet aux clients d'envoyer des conseils génériques de transposition d'utilisateur dans un message de prise de contact de données supplémentaires défini dans la RFC 4680. Un tel conseil de transposition est défini dans une section informative, UpnDomainHint, qui peut être utilisé par un serveur pour localiser un utilisateur dans un répertoire. D'autres conseils de transposition pourront être définis dans d'autres documents à l'avenir.

Table des matières

1. Introduction

Le présent document a une partie normative et une partie pour information. Les sections 2 à 5 sont normatives. La Section 6 est pour information.

La présente spécification définit une extension à TLS et une charge utile pour le message de prise de contact SupplementalData *(données supplémentaires)* défini dans la [RFC4680], pour traiter la transposition des utilisateurs en leur compte d'utilisateur quand ils utilisent l'authentification de client TLS comme méthode d'authentification.

La nouvelle extension TLS (user_mapping) *(transposition d'utilisateur)* est envoyée dans le message hello du client. Selon la convention définie dans la [RFC4366], le serveur place la même extension (user_mapping) dans le message hello de serveur, pour informer le client que le serveur comprend cette extension. Si le serveur ne comprend pas l'extension, il va répondre avec un hello de serveur qui omet cette extension, et le client va poursuivre comme d'habitude, en ignorant l'extension, et sans inclure de données de UserMappingDataList *(liste de données de transposition d'utilisateur)* dans la prise de contact TLS.

Si la nouvelle extension est comprise, le client va injecter les données de UserMappingDataList dans le message

SupplementalData de prise de contact avant le message Certificat de client. Le serveur va alors analyser ce message, extraire le domaine du client, et le mémoriser dans le contexte pour l'utiliser lors de la transposition du certificat en le compte de répertoire de l'utilisateur.

Aucune autre modification n'est requise du protocole. Les messages sont détaillés dans les sections suivantes.

1.1 Terminologie

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

La syntaxe de l'extension Transposition d'utilisateur TLS est définie en utilisant le langage de présentation de TLS, qui est spécifié à la Section 4 de la [RFC2246].

1.2 Considérations de conception

La raison pour laquelle la transposition des données n'est pas elle-même placée dans la portion extension du hello de client est d'empêcher la diffusion de ces informations aux serveurs qui ne comprennent pas l'extension.

2. Extension Transposition d'utilisateur

Un nouveau type d'extension (user_mapping(6)) est ajouté à l'extension utilisée dans les messages hello de client et hello de serveur. Le type d'extension est spécifié comme suit.

```
enum {
    user_mapping(6), (65535)
} ExtensionType;
```

Le champ "extension_data" de cette extension DEVRA contenir "UserMappingTypeList" avec une liste des types de conseils pris en charge où :

```
struct {
     UserMappingType user_mapping_types<1..2^8-1>;
} UserMappingTypeList;
```

L'énumération des types de conseils (user_mapping_types) définis dans le présent document est fournie à la Section 3.

La liste des user_mapping_types *(types de transposition d'utilisateur)* incluse dans un hello de client DEVRA signaler les types de conseils pris en charge par le client. La liste des user_mapping_types incluse dans le hello de serveur DEVRA signaler les types de conseils préférés par le serveur.

Si aucun des types de conseils figurant sur la liste du client n'est pris en charge par le serveur, le serveur DEVRA omettre l'extension user_mapping dans le hello de serveur.

Quand l'extension user_mapping est incluse dans le hello de serveur, la liste des types de conseils dans "UserMappingTypeList" DEVRA être soit égale à la liste, soit à un sous ensemble de la liste fournie par le client.

3. Échange de prise de contact de transposition d'utilisateur

La structure sous-jacente du message SupplementalData de prise de contact, utilisé pour porter les informations définies dans cette section, est définie dans la [RFC4680].

Un nouveau SupplementalDataType [RFC4680] est défini pour traiter la communication de données génériques de transposition d'utilisateur. Voir dans TLS 1.0 [RFC2246] et TLS 1.1 [RFC4346] les autres types de prise de contact.

Les informations dans ce type de données portent un ou plusieurs conseils non authentifiés, UserMappingDataList, insérés par le côté client. À réception et achèvement réussi de la prise de contact TLS, le serveur PEUT utiliser ce conseil pour localiser le compte de l'utilisateur d'où les informations et accréditifs d'utilisateur PEUVENT être restitués pour prendre en charge l'authentification fondée sur le certificat du client.

```
struct {
    SupplementalDataType supp_data_type;
    uint16 supp_data_length;
    select(SupplementalDataType) {
      case user_mapping_data: UserMappingDataList;
      }
} SupplementalDataEntry;

enum {
    user_mapping_data(0), (65535)
} SupplementalDataType;
```

L'énumération user_mapping_data(0) résulte en un nouveau type de données supplémentaires UserMappingDataList avec la structure suivante :

```
enum {
    (255)
} UserMappingType;

struct {
     UserMappingType user_mapping_version;
     uint16 user_mapping_length;
     select(UserMappingType) { }
} UserMappingData;

struct{
  UserMappingData user_mapping_data_list<1..2^16-1>;
}UserMappingDataList;
```

user_mapping_length
Ce champ est la longueur (en octets) des données choisies par UserMappingType.

La structure UserMappingData contient une seule transposition du type UserMappingType. Cette structure peut être utilisée pour définir de nouveaux types de conseils de transposition d'utilisateur à l'avenir. La UserMappingDataList PEUT porter plusieurs conseils ; elle est définie comme un vecteur de structures UserMappingData.

Aucune préférence n'est donnée à l'ordre dans lequel les conseils sont spécifiés dans ce vecteur. Si le client envoie plus d'un conseil, le serveur DEVRAIT alors utiliser la transposition applicable prise en charge par le serveur.

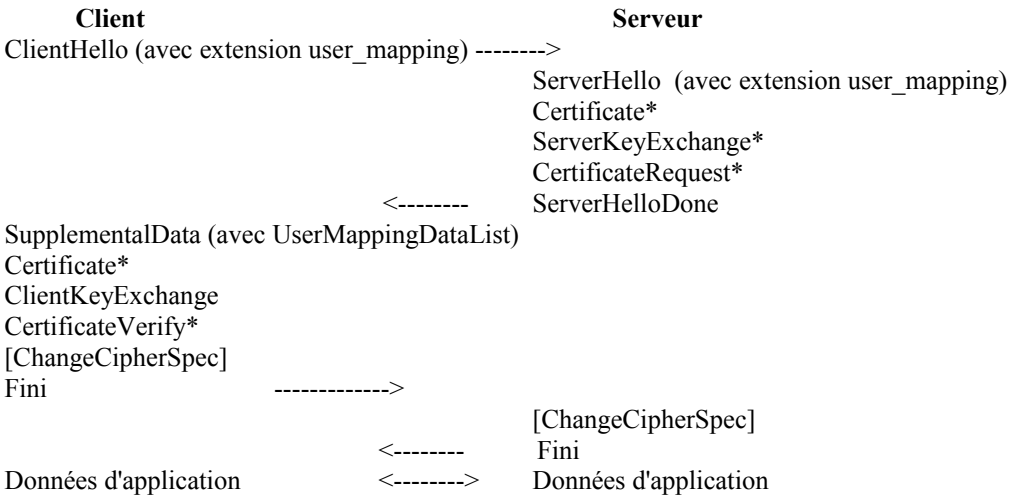
Les mises en œuvre PEUVENT prendre en charge le conseil de domaine UPN comme spécifié à la Section 6 du présent document. Les mises en œuvre PEUVENT aussi prendre en charge d'autres types de transposition d'utilisateur lorsque il en est défini. Les définitions de types de transposition d'utilisateur sur la voie de la normalisation doivent inclure une discussion des considérations d'internationalisation.

4. Flux de messages

Afin de négocier l'envoi de données de transposition d'utilisateur à un serveur en accord avec la présente spécification, les clients DOIVENT inclure une extension du type "user_mapping" dans le client hello (étendu) qui DEVRA contenir une liste des types de conseils pris en charge.

Les serveurs qui reçoivent un hello de client étendu contenant une extension "user_mapping" PEUVENT indiquer qu'ils veulent accepter les données de transposition d'utilisateur en incluant une extension de type "user_mapping" dans le hollo (étendu) de serveur, qui DEVRA contenir une liste des types de conseils préférés.

Après que la négociation de l'utilisation de la transposition d'utilisateur a été achevée avec succès (par l'échange des messages hello incluant les extensions "user_mapping") les clients PEUVENT envoyer un message "SupplementalData" contenant la "UserMappingDataList" avant le message "Certificate". Le flux de messages est illustré à la Figure 1.



* Indique des messages facultatifs ou dépendants de la situation qui ne sont pas toujours envoyés selon la [RFC2246] et la [RFC4346].

Figure 1. Flux de messages avec données de transposition d'utilisateur

Le serveur DOIT s'attendre, et traiter en douceur, le cas où le client choisit de ne pas envoyer de message supplementalData de prise de contact même après une négociation réussie des extensions. Le client PEUT à sa discrétion décider que le conseil de transposition d'utilisateur qu'il avait initialement l'intention d'envoyer n'est plus pertinent pour cette session. Une raison pourrait être que le certificat du serveur ne satisfait pas à certaines exigences.

5. Considérations sur la sécurité

Le conseil de transposition d'utilisateur envoyé dans la UserMappingDataList n'est pas authentifié et NE DOIT PAS être traité comme un identifiant de confiance. L'authentification de l'utilisateur représentée par ce conseil de transposition d'utilisateur DOIT s'appuyer seulement sur la validation du certificat de client. Une façon de le faire est d'utiliser le conseil de transposition d'utilisateur pour localiser et extraire du répertoire de confiance un certificat du prétendu utilisateur et de confronter ensuite ce certificat au certificat validé du client dans la prise de contact TLS.

Comme le client est l'initiateur de cette extension TLS, il a besoin de déterminer quand il est approprié d'envoyer les informations de transposition d'utilisateur. Il peut n'être pas prudent de diffuser un conseil de transposition d'utilisateur à juste un serveur à un moment donné.

Pour éviter d'envoyer des conseils de transposition d'utilisateur superflus, les clients DEVRAIENT seulement envoyer ces informations si ils reconnaissent le serveur comme un receveur légitime. La reconnaissance du serveur peut être faite de nombreuses façons. Une d'elles pourrait être de reconnaître le nom et l'adresse du serveur.

Dans certains cas, le conseil de transposition d'utilisateur peut lui-même être regardé comme sensible. Dans ce cas, la technique de double prise de contact décrite dans la [RFC4680] peut être utilisée pour assurer la protection des informations de conseil de transposition d'utilisateur.

6. Conseil de domaine UPN (information)

La présente spécification donne pour information une description d'un type de conseil de transposition d'utilisateur pour les conseils de nom de domaine et les conseils de nom principal d'utilisateur. D'autres types de conseils pourront être définis dans d'autres documents futurs.

Le nom principal d'utilisateur (UPN, *User Principal Name*) dans ce type de conseil représente un nom qui spécifie une entrée d'un utilisateur dans un répertoire sous la forme de nomD'utilisateur@nomDeDomaine. Traditionnellement, Microsoft s'est appuyé sur la présence d'une telle forme de nom dans le certificat de client certificat lors de la connexion à un compte de domaine. Cependant, ceci a plusieurs inconvénients car cela empêche l'utilisation de certificats avec un UPN absent et exige aussi la reproduction des certificats ou la production de plusieurs certificats pour refléter les changements de comptes ou la création de nouveaux comptes. L'extension TLS, combinée avec le type de conseil défini, apporte une amélioration significative à cette situation car elle permet qu'un seul certificat soit transposé en un ou plusieurs comptes de l'utilisateur et n'exige pas que le certificat contienne un UPN de propriétaire.

Le champ domain_name PEUT être utilisé quand seulement l'information du domaine est nécessaire, par exemple, si un utilisateur a des comptes dans plusieurs domaines en utilisant le même nom d'utilisateur, si ce nom d'utilisateur est connu par une autre source (par exemple, le certificat du client). Quand le nom d'utilisateur est aussi nécessaire, le champ user_principal_name PEUT être utilisé pour indiquer à la fois le nom d'utilisateur et le nom de domaine. Si les deux champs sont présents, alors le serveur peut utiliser celui de son choix.

```
enum {
    upn_domain_hint(64), (255)
} UserMappingType;

struct {
    opaque user_principal_name<0..2^16-1>;
    opaque domain_name<0..2^16-1>;
} UpnDomainHint;

struct {
    UserMappingType user_mapping_version;
    uint16 user_mapping_length;
    select(UserMappingType) {
        case upn_domain_hint: UpnDomainHint;
    }
} UserMappingData;
```

Le champ user_principal_name, quand il est spécifié, DEVRA être de la forme "utilisateur@domaine", où "utilisateur" est une chaîne Unicode codée en UTF-8 qui ne contient pas le caractère "@", et "domaine" est un nom de domaine satisfaisant aux exigences du paragraphe qui suit.

Le champ domain_name, quand il est spécifié, DEVRA contenir un nom de domaine [RFC1034] dans la forme usuelle text ; en d'autres termes, une séquence de une ou plusieurs étiquettes de domaine séparées par ".", chaque étiquette de domaine commençant et se terminant par un caractère alphanumérique et contenant éventuellement aussi des caractères "-". Ce champ est un "intervalle de nom de domaine sans capacité IDN" comme défini dans la [RFC3490], et donc, les noms de domaines contenant des caractères non ASCII doivent être traités comme décrit dans la RFC 3490 avant d'être mémorisés dans ce champ.

Le conseil UpnDomainHint DOIT au moins contenir un user_principal_name non vide ou un domain_name non vide. Le conseil UpnDomainHint PEUT contenir les deux user_principal_name et domain_name.

7. Considérations relatives à l'IANA

IANA a effectué les actions suivantes :

1) Créé une entrée, user_mapping(6), dans le registre existant pour ExtensionType (défini dans la [RFC4366]).

2) Créé une entrée, user_mapping_data(0), dans le nouveau registre pour SupplementalDataType (défini dans la RFC4680).

3) Établi un registre pour les valeurs TLS de UserMappingType. La première entrée dans le registre est upn_domain_hint(64). Les valeurs TLS de UserMappingType dans la gamme inclusive de 0 à 63 (décimal) sont allouées via l'action de normalisation de la [RFC2434]. Les valeurs de la gamme inclusive de 64 à 223 (décimal) sont allouées via la spécification exigée de la [RFC2434]. Les valeurs de la gamme inclusive 224 à 255 (décimal) sont réservées pour utilisation privée de la [RFC2434].

8. Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

[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)

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

[RFC4366] S. Blake-Wilson et autres, "Extensions de sécurité de la couche Transport (TLS)", avril 2006. (*Obsolète,* RFC5246) *(P.S.)*

[RFC4680] S. Santesson, "Message de prise de contact TLS pour données supplémentaires", octobre 2006. (*MàJ* RFC4346) *(P.S.)*

9. Remerciements

Les auteurs remercient tout particulièrement Russ Housley, Eric Resocorla, et Paul Leach de leurs substantielles contributions.

Adresse des auteurs

Stefan Santesson
Microsoft
Finlandsgatan 30
164 93 KISTA
Sweden
mél : stefans@microsoft.com

Ari Medvinsky
Microsoft
One Microsoft Way
Redmond, WA 98052-6399
USA
mél : arimed@microsoft.com

Joshua Ball
Microsoft
One Microsoft Way
Redmond, WA 98052-6399
USA
mél : joshball@microsoft.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

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

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

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

Remerciement

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