Groupe de travail Réseau
Request for Comments : 4680
RFC mise à jour : 4346
Catégorie : Sur la voie de la normalisation

S. Santesson, Microsoft
septembre 2006

Traduction Claude Brière de L'Isle

Message de prise de contact TLS pour données supplémentaires

Résumé
La présente spécification définit un message de prise de contact TLS pour échanger des données supplémentaires d'application. Les extensions du message hello TLS sont utilisées pour déterminer quels types de données supplémentaires sont prises en charge par à la fois le client et le serveur TLS. Ensuite le messages de prise de contact de données supplémentaires est utilisé pour échanger les données. D'autres documents définiront la syntaxe de ces extensions et la syntaxe des types de données supplémentaires associés.

Table des matières

1. Introduction

De récentes activités de normalisation ont proposé différents mécanismes pour transmettre des données d'application supplémentaires dans le message d'échange TLS. Par exemple, des propositions récentes transfèrent des données qui ne sont pas traitées par le protocole TLS lui-même, mais aident l'application protégée par TLS dans les décisions d'authentification et d'autorisation. Une proposition transfère des indications de nom d'utilisateur pour localiser les accréditifs, et une autre proposition transfère les certificats d'attribut et les assertions en langage de balisage d'assertions de sécurité (SAML, *Security Assertions Markup Language*) pour les vérifications d'autorisation.

Afin d'éviter la définition de plusieurs messages de prise de contact, un pour chaque nouveau type de données supplémentaires spécifiques d'application, la présente spécification définit un nouveau type de message de prise de contact qui regroupe tous les objets de données qui sont à livrer à l'application protégée par TLS et les envoie dans un seul message de prise de contact.

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 du message de prise de contact supplemental_data est définie en utilisant le langage de présentation de TLS, qui est spécifié à la Section 4 de la [RFC2246].

2. Message de prise de contact Données supplémentaires

Le nouveau type de message de prise de contact supplemental_data est défini pour s'accommoder de la communication des objets de données supplémentaires qui ont fait l'objet d'un accord durant l'échange des extensions dans les messages hello du client et du serveur. Voir dans la [RFC2246] (TLS 1.0) et la [RFC4346] (TLS 1.1) les autres types de message de prise de contact.

Les informations fournies dans un objet de données supplémentaires DOIVENT être destinées à être utilisées exclusivement par les applications et protocoles au-dessus de la couche de protocole TLS. De telles données NE DOIVENT PAS avoir besoin d'être traitées par le protocole TLS.

```
enum {
     supplemental_data(23), (255)
  } HandshakeType;

struct {
     HandshakeType msg_type;                    /* type de prise de contact */
     uint24 length;                             /* octets dans le message */
     select (HandshakeType) {
          case supplemental_data:   SupplementalData;
       } body;
   } Handshake;

struct {
     SupplementalDataEntry supp_data<1..2^24-1>;
  } SupplementalData;

struct {
     SupplementalDataType supp_data_type;
     uint16 supp_data_length;
     select(SupplementalDataType) { }
  } SupplementalDataEntry;

enum {
     (65535)
  } SupplementalDataType;
```

supp_data_length
Ce champ est la longueur (en octets) des données choisies par SupplementalDataType.

Le client NE DOIT PAS envoyer plus d'un message de prise de contact SupplementalData, et le serveur NE DOIT PAS envoyer plus d'un message de prise de contact SupplementalData. Recevoir plus d'un message de prise de contact SupplementalData résulte en une erreur fatale, et le receveur DOIT clore la connexion avec une alerte fatale unexpected_message *(message inattendu)*.

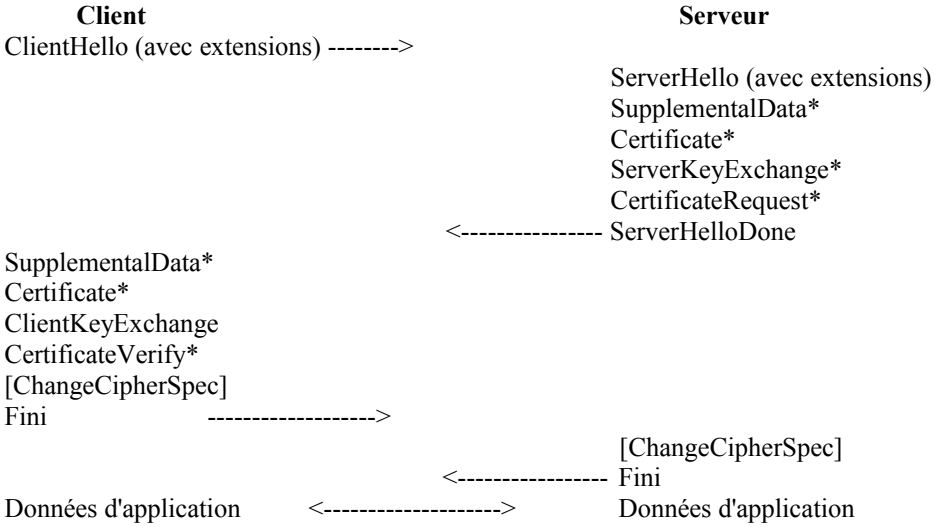
Si il est présent, le message de prise de contact SupplementalData DOIT contenir une structure non vide SupplementalDataEntry portant les données associées avec au moins un SupplementalDataType défini. Un accord explicite qui gouverne la présence de toutes données supplémentaires DOIT être conclu entre le client et le serveur pour chaque SupplementalDataType utilisant les extensions TLS [RFC4366] dans les messages hello de client et de serveur. La réception d'un message de prise de contact SupplementalData inattendu résulte en une erreur fatale, et le receveur DOIT clore la connexion avec une alerte fatale unexpected_message.

D'autres documents définiront les types spécifiques de données supplémentaires et la syntaxe et traitement de données associés. Ces mêmes spécifications doivent aussi spécifier les extensions de message hello de client et de serveur qui sont utilisées pour négocier la prise en charge du type de données supplémentaires spécifié. Le présent document spécifie simplement le message de protocole de prise ce contact TLS qui va porter les objets de données supplémentaires.

Différentes situations exigent le transfert de données supplémentaires du client au serveur, exigent le transfert de données supplémentaires du serveur au client, ou dans les deux sens. Ces situations sont toutes trois pleinement prises en charge.

3. Flux de messages

Le message de prise de contact SupplementalData, si il est échangé, DOIT être envoyé comme premier message de prise de contact, comme illustré dans la Figure 1 ci-dessous.



* Indique un message facultatif ou qui dépend de la situation.

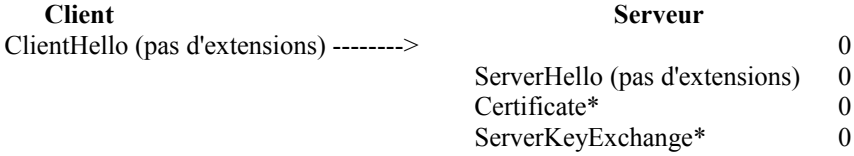
Figure 1. Flux de messages avec SupplementalData

4. Considérations sur la sécurité

Chaque type de données supplémentaires inclus dans le message de prise de contact défini dans la présente spécification introduit son propre ensemble unique de propriétés de sécurité et les considérations qui s'y rapportent. Les considérations de sécurité doivent donc être définies dans chaque document qui définit un type de données supplémentaire.

Dans certains cas, les informations de données supplémentaires peuvent être sensibles. La technique de double prise de contact peut être utilisée pour assure la protection des informations de données supplémentaires. La Figure 2 illustre la double prise de contact, où la prise de contact initiale n'inclut aucune extension, mais résulte en des communications protégées. Ensuite, une seconde prise de contact qui inclut les informations de SupplementalData est effectuée en utilisant les communications protégées. Dans la Figure 2, le nombre sur la droite indique la quantité de protection pour le message TLS sur cette ligne. Un zéro (0) indique qu'il n'y a pas de protection de la communication ; un un (1) indique que la protection est fournie par la première session TLS ; et un deux (2) indique que la protection est fournie par les deux sessions TLS.

Le placement du message SupplementalData dans la prise de contact TLS résulte en ce que le serveur fournit ses informations de SupplementalData avant que le client soit authentifié. Dans de nombreuses situations, les serveurs ne vont pas vouloir fournir des informations d'autorisation tant que le client n'est pas authentifié. La double prise de contact illustrée à la Figure 2 donne une technique pour s'assurer que les parties sont mutuellement authentifiées avant que l'une ou l'autre partie ait fourni les informations de données supplémentaires.



```
                                  CertificateRequest*              0
                         <--------ServerHelloDone                  0
Certificate*                                                       0
ClientKeyExchange                                                  0
CertificateVerify*                                                 0
[ChangeCipherSpec]                                                 0
Finished                 -------->                                 1
                                  [ChangeCipherSpec]               0
                         <--------Fini                             1
ClientHello (w/ extensions) -------->                              1
                                  ServerHello (avec extensions)    1
                                  SupplementalData*                1
                                  Certificate*                     1
                                  ServerKeyExchange*               1
                                  CertificateRequest*              1
                         <--------ServerHelloDone                  1
SupplementalData*                                                  1
Certificate*                                                       1
ClientKeyExchange                                                  1
CertificateVerify*                                                 1
[ChangeCipherSpec]                                                 1
Fini                     -------->                                 2
                                  [ChangeCipherSpec]               1
                         <--------Fini                             2
Données d'application    <-------->Données d'application           2
```

* Indique un message facultatif ou qui dépend de la situation.

Figure 2. Double prise de contact pour protéger les données supplémentaires

5. Considérations relatives à l'IANA

L'IANA a effectué les actions suivantes :

1) Créé une entrée, supplemental_data(23), dans le registre existant pour HandshakeType (défini dans la [RFC2246]).

2) Établi un registre pour les formats de données supplémentaires TLS (SupplementalDataType). Les valeurs incluses dans la gamme de 0 à 16385 (décimal) sont allouées via action de normalisation selon la [RFC2434]. Les valeurs dans la gamme 16386 à 65279 (décimal) sont allouées via le consensus de l'IETF de la [RFC2434]. Les valeurs dans la gamme 65280 à 65535 (décimal) sont réservée pour utilisation privée de la RFC 2434.

6. Références normatives

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

[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)

[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, voir la* RFC5246) *(P.S.)*

7. Remerciements

L'idée architecturale fondamentale du message de données supplémentaires de prise de contact a été fournie par Russ Housley et Eric Rescorla.

Adresse de l'auteur

Stefan Santesson
Microsoft
Finlandsgatan 30
164 93 KISTA
Sweden

mél : stefans@microsoft.com

Déclaration complète de droits de reproduction

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