

Groupe de travail Réseau
Request for Comments : 2659
Catégorie : Expérimentale
Traduction Claude Brière de L'Isle

E. Rescorla, RTFM, Inc.
A. Schiffman, Terisa Systems, Inc.
août 1999

Extensions de sécurité pour HTML

Statut de ce mémoire

Le présent mémoire définit un protocole expérimental pour la communauté de l'Internet. Il ne spécifie en aucune façon une norme de l'Internet. Des discussions et des suggestions pour son amélioration sont demandées. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (1999). Tous droits réservés

Résumé

Le présent mémoire décrit une syntaxe pour incorporer les paramètres de négociation S-HTTP dans les documents HTML. S-HTTP, comme décrit dans la RFC 2660, contient le concept d'en-têtes de négociation qui reflètent les préférences du receveur potentiel d'un message à l'égard des améliorations cryptographiques qui devraient être appliquées au message. Le présent document décrit une syntaxe pour lier ces paramètres de négociation aux ancres HTML.

1. Introduction

2. Attributs d'ancres

On définit les nouveaux attributs d'ancres (et leur formulaire de soumission) suivants :

DN Le nom distinctif du principal pour lequel la demande devrait être chiffrée lorsque on déréfère l'url de l'ancre. Il n'a pas besoin d'être spécifié, mais manquer à le faire fait courir le risque que le client soit incapable de déterminer le DN et donc soit incapable de chiffrer. Cela devrait être spécifié dans la forme de la RFC1485, en utilisant si nécessaire les conventions de citation de SGML.

NONCE Chaîne de format libre (citée de façon appropriée en SGML) qui est à inclure dans un en-tête SHTTP-Nonce: (après le retrait de la citation SGML) lorsque l'ancre est déréférée.

CRYPTOPTS Informations d'option cryptographique comme décrites dans [SHTTP]. Précisément, la production <cryptopt-list>.

2.1 Élément CERTS

Un nouvel élément CERTS HTML est défini, qui porte un groupe (pas nécessairement en rapport) de certificats fourni comme données de conseil. Le contenu des éléments n'est pas destiné à l'affichage à l'utilisateur. Les groupes de certificats peuvent être fournis d'une façon appropriée pour les mises en œuvre de PEM ou PKCS-7. De tels certificats sont fournis dans le document HTML pour l'agrément du receveur, qui pourrait autrement être incapable de restituer le certificat (ou la chaîne de certificats) correspondant à un DN spécifié dans une ancre.

Le format devrait être le même que celui de la ligne d'en-tête 'Certificate-Info' de la [RFC2660] excepté que le spécificateur <Cert-Fmt> devrait être fourni comme attribut FMT dans l'étiquette.

Plusieurs éléments CERTS sont permis ; il est suggéré que les éléments CERTS eux-mêmes soient inclus dans l'élément HEAD du document HTML (dans l'espoir que les données ne seront pas affichées par des navigateurs sans S-HTTP mais conformes à HTML.)

2.2 Élément CRYPTOPTS

Cryptopts peut aussi être éclaté en un élément et référencé dans une ancre par son nom. L'attribut NAME spécifie le nom par lequel cet élément peut être référencé dans un attribut CRYPTOPTS dans une ancre. Les noms doivent avoir un # comme premier caractère.

2.3 Exemple HTML

Un exemple de données cryptographiques incorporées dans une ancre, traitées par un groupe de certificats est fourni ci-dessous. Noter que la syntaxe de citation SGML est utilisée pour fournir les marques de citation incorporées.

```
<CERTS FMT=PKCS-7>
MIAGCSqGSIb3DQEHAqCAMIACAQExADCABgkqhkiG9w0BBwEAAKCAMIIBrTCCAUKAgC2MA0GCSqGSIb3DQ
EBAgUAME0xCzAJBgNVBAYTAIVTMSAwHgYDVQQKEXdSU0EgRGF0YSBTZWN1cmI0eSwgSW5jLjEcmBoGA1UE
CxMTUGVyc29uYSBDZXJ0aWZpY2F0ZTAeFw05NDA0MDkwMDUwMzdaFw05NDA4MDIxODM4NTdaMGcxZzAJBg
NVBAYTAIVTMSAwHgYDVQQKEXdSU0EgRGF0YSBTZWN1cmI0eSwgSW5jLjEcmBoGA1UECxMTUGVyc29uYSBD
ZXJ0aWZpY2F0ZTEYMBYGA1UEAxMPU2V0ZWNgQXN0cm9ub215MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
AMy8QcW7RMrB4sTdQ8Nmb2DFmJmkWn+eI+NdeamIDEIX/qw9mIQu4xNj1FfepfJNxzPvA00tMKhy6+bkrlyMEU8CAw
EAATANBgkqhkiG9w0BAQIFAANPAAYn7jDgirhiIL4wnP8nGzUisGSpsFsF4/7z2P2wqne6Qk8Cg/Dstu3RyaN78vAMGP8d
82H5+Ndfhi2mRp4YHiGHZ0HIK6VbPfinyS2wdjCCAccwggFRAGUCQAAAFDANBgkqhkiG9w0BAQIFADBfMQswCQY
DVQQQEwJVUzEgMB4GA1UEChMXUINBIERhdGEgU2VjdXJpdHksIEluYy4xLjAsBgNVBAsTJUxvdyBBc3N1cmFuY2
UgQ2VydGlmaWNhdGlvbiBBdXR0b3JpdHkwHhcNOTQwMTA3MDAwMDAwWhcNOTYwMTA3MjM1OTU5WjBNMQs
wCQYDVQQGEwJVUzEgMB4GA1UEChMXUINBIERhdGEgU2VjdXJpdHksIEluYy4xLjAsBgNVBAsTE1BlcnNvbmEg
Q2VydGlmaWNhdGUwaTANBgkqhkiG9w0BAQEFAANYADBVAK4GqghQDa9Xi/2zAdYEqJVlcYh1LN1FpI9tXQ1m6zZ3
9PYXK8Uhoj0Es7kWRv8hC04vqkOKwndWbzVtvoHQOmP8nOkkuBi+AQvgFoRcgOUCAwEAATANBgkqhkiG9w0BAQI
FAANhAD/5Uo7xDdp49oZm9GoNcPhZcW1e+nojLvHXWAU/CBkwfR+FSf4hQ5eFu1AjYv6Wqf430Xe9Et5+jgnMTiq4Ln
wgTdA8xQX4eIjz9QzQobkE3XVOjVAAtCFcmiin80RB8AAAMYAAAAAAA
AAAAA==
</CERTS>
<Un nom=foobar
DN="CN=Setec Astronomy, OU=Persona Certificate,
O="&quot;RSA Data Security, Inc.&quot;; C=US"
CRYPTOPTS="SHTTP-Privacy-Enhancements: recv-refused=encrypt;
SHTTP-Signature-Algorithms: recv-required=NIST-DSS"
HREF="shttp://research.nsa.gov/skipjack-holes.html">
Ne pas lire ceci. </A>
```

3. Considérations sur la sécurité

Ce document tout entier traite de la sécurité.

4. Adresse des auteurs

Eric Rescorla
RTFM, Inc.
30 Newell Road, #16
East Palo Alto, CA 94303
téléphone : (650) 328-8631
mél : ekr@rtfm.com

Allan M. Schiffman
SPYRUS/Terisa
5303 Betsy Ross Drive
Santa Clara, CA 95054
téléphone : (408) 327-1901
mél : ams@terisa.com

5. Références

[RFC2660] E. Rescorla, et A. Schiffman, "[Protocole de transfert HyperTexte sécurisé](#)", août 1999. (*Expérimentale*)

6. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

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