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

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 déréférence 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 déréférencée.

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 certaificat (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 dns 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 fournie les marques de citation incorporées.

<CERTS FMT=PKCS-7>
MIAGCSqGSIb3DQEHAqCAMIACAQExADCABgkqhkiG9w0BBwEAAKCAMIIBrTCCAUkCAgC2MA0GCSqGSIb3DQ
EBAgUAME0xCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5jLjEcMBoGA1UE
CxMTUGVyc29uYSBDZXJ0aWZpY2F0ZTAeFw05NDA0MDkwMDUwMzdaFw05NDA4MDIxODM4NTdaMGcxCzAJBg
NVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5jLjEcMBoGA1UECxMTUGVyc29uYSBD
ZXJ0aWZpY2F0ZTEYMBYGA1UEAxMPU2V0ZWMgQXN0cm9ub215MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
AMy8QcW7RMrB4sTdQ8Nmb2DFmJmkWn+el+NdeamIDElX/qw9mIQu4xNj1FfepfJNxzPvA0OtMKhy6+bkrlyMEU8CAw
EAATANBgkqhkiG9w0BAQIFAANPAAYn7jDgirhiIL4wnP8nGzUisGSpsFsF4/7z2P2wqne6Qk8Cg/Dstu3RyaN78vAMGP8d
82H5+Ndfhi2mRp4YHiGHz0HlK6VbPfnyvS2wdjCCAccwggFRAgUCQAAAFDANBgkqhkiG9w0BAQIFADBfMQswCQY
DVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhdGEgU2VjdXJpdHksIEluYy4xLjAsBgNVBAsTJUxvdyBBc3N1cmFuY2
UgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNOTQwMTA3MDAwMDAwWhcNOTYwMTA3MjM1OTU5WjBNMQs
wCQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhdGEgU2VjdXJpdHksIEluYy4xHDAaBgNVBAsTE1BlcnNvbmEg
Q2VydGlmaWNhdGUwaTANBgkqhkiG9w0BAQEFAANYADBVAk4GqghQDa9Xi/2zAdYEqJVIcYhlLN1FpI9tXQ1m6zZ3
9PYXK8Uhoj0Es7kWRv8hC04vqkOKwndWbzVtvoHQOmP8nOkkuBi+AQvgFoRcgOUCAwEAATANBgkqhkiG9w0BAQI
FAANhAD/5Uo7xDdp49oZm9GoNcPhZcW1e+nojLvHXWAU/CBkwfcR+FSf4hQ5eFu1AjYv6Wqf430Xe9Et5+jgnMTiq4Ln
wgTdA8xQX4elJz9QzQobkE3XVOjVAtCFcmiin80RB8AAAMYAAAAAA
AAAAA==
</CERTS>
<Un nom=foobar
DN="CN=Setec Astronomy, OU=Persona Certificate,
O="RSA Data Security, Inc.", 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

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