Network Working Group
Requests for Comments: 2659
Category: Experimental

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

August 1999

Security Extensions For HTML

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This memo describes a syntax for embedding S-HTTP negotiation parameters in HTML documents. S-HTTP, as described by RFC 2660, contains the concept of negotiation headers which reflect the potential receiver of a message's preferences as to which cryptographic enhancements should be applied to the message. This document describes a syntax for binding these negotiation parameters to HTML anchors.

1. Introduction

2. Anchor Attributes

We define the following new anchor (and form submission) attributes:

DN -- The distinguished name of the principal for whom the request should be encrypted when dereferencing the anchor's url. This need not be specified, but failure to do so runs the risk that the client will be unable to determine the DN and therefore will be unable to encrypt. This should be specified in the form of RFC1485, using SGML quoting conventions as needed.

NONCE -- A free-format string (appropriately SGML quoted) which is to be included in a SHTTP-Nonce: header (after SGML quoting is removed) when the anchor is dereferenced.

CRYPTOPTS -- Cryptographic option information as described in

[SHTTP]. Specifically, the <cryptopt-list> production.

2.1. CERTS Element

A new CERTS HTML element is defined, which carries a (not necessarily related) group of certificates provided as advisory data. The element contents are not intended to be displayed to the user. Certificate groups may be provided appropriate for either PEM or PKCS-7 implementations. Such certificates are supplied in the HTML document for the convenience of the recipient, who might otherwise be unable to retrieve the certificate (chain) corresponding to a DN specified in an anchor.

The format should be the same as that of the 'Certificate-Info' header line, of [SHTTP] except that the <Cert-Fmt> specifier should be provided as the FMT attribute in the tag.

Multiple CERTS elements are permitted; it is suggested that CERTS elements themselves be included in the HTML document's HEAD element (in the hope that the data will not be displayed by S-HTTP oblivious but HTML compliant browsers.)

2.2. CRYPTOPTS Element

Cryptopts may also be broken out into an element and referred to in anchors by name. The NAME attribute specifies the name by which this element may be referred to in a CRYPTOPTS attribute in an anchor. Names must have a # as the leading character.

2.3. HTML Example

An example of cryptographic data embedded in an anchor, proceeded by a certificate group is provided below. Note the SGML quoting syntax used to supply embedded quotation marks.

```
<CERTS FMT=PKCS-7>
MIAGCSqGSIb3DQEHAqCAMIACAQExADCABgkqhkiG9w0BBwEAAKCAM
IIBrTCCAUkCAgC2MA0GCSqGSIb3DQEBAgUAME0xCzAJBgNVBAYTAlVTMSAwH
gYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5jLjEcMBoGA1UECxMTUGVyc
29uYSBDZXJ0aWZpY2F0ZTAeFw05NDA0MDkwMDUwMzdaFw05NDA4MDIxODM4N
TdaMGcxCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0e
SwgSW5jLjEcMBoGA1UECxMTUGVyc29uYSBDZXJ0aWZpY2F0ZTEYMBYGA1UEA
xMPU2V0ZWMgQXN0cm9ub215MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMy8Q
cW7RMrB4sTdQ8Nmb2DFmJmkWn+el+NdeamIDElX/qw9mIQu4xNj1FfepfJNx
zPvA0OtMKhy6+bkrlyMEU8CAwEAATANBgkqhkiG9w0BAQIFAANPAAYn7jDgi
rhiIL4wnP8nGzUisGSpsFsF4/7z2P2wqne6Qk8Cg/Dstu3RyaN78vAMGP8d8
2H5+Ndfhi2mRp4YHiGHz0HlK6VbPfnyvS2wdjCCAccwggFRAgUCQAAAFDANB
gkqhkiG9w0BAQIFADBfMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhd
```

```
GEgU2VjdXJpdHksIEluYy4xLjAsBgNVBAsTJUxvdyBBc3N1cmFuY2UgQ2Vyd
GlmaWNhdGlvbiBBdXRob3JpdHkwHhcNOTQwMTA3MDAwMDAwWhcNOTYwMTA3M
jM1OTU5WjBNMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhdGEgU2Vjd
XJpdHksIEluYy4xHDAaBgNVBAsTE1BlcnNvbmEgQ2VydGlmaWNhdGUwaTANB
gkqhkiG9w0BAQEFAANYADBVAk4GqghQDa9Xi/2zAdYEqJVIcYhlLN1FpI9tX
Q1m6zZ39PYXK8Uhoj0Es7kWRv8hC04vqkOKwndWbzVtvoHQOmP8nOkkuBi+A
QvgFoRcgOUCAwEAATANBgkqhkiG9w0BAQIFAANhAD/5Uo7xDdp49oZm9GoNc
PhZcW1e+nojLvHXWAU/CBkwfcR+FSf4hQ5eFu1AjYv6Wqf430Xe9Et5+jgnM
Tiq4LnwgTdA8xQX4elJz9QzQobkE3XVOjVAtCFcmiin80RB8AAAMYAAAAAAA
AAAAA==
</CERTS>
<A name=foobar
DN="CN=Setec Astronomy, OU=Persona Certificate,
    O=&amp;quot;RSA Data Security, Inc.&amp;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">
Don’t read this. </A>
```

3. Security Considerations

This entire document is about security.

4. Authors’ Addresses

Eric Rescorla
RTFM, Inc.
30 Newell Road, #16
East Palo Alto, CA 94303

Phone: (650) 328-8631
EMail: ekr@rtfm.com

Allan M. Schiffman
SPYRUS/Terisa
5303 Betsy Ross Drive
Santa Clara, CA 95054

Phone: (408) 327-1901
EMail: ams@terisa.com

5. References

[SHTTP] Rescorla, E. and A. Schiffman, "The Secure HyperText Transfer Protocol", RFC 2660, August 1999.

6. Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.