Network Working Group
Requests for Comments: 2659
Category: Experimental

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

August 1999

Защитные расширения для HTML

Security Extensions For HTML

Статус документа

Этот документ определяет экспериментальный протокол для сообщества Internet. Документ не задает каких-либо стандартов Internet. Принимаются предложения и комментарии к документу. Документ может распространяться без ограничений.

Авторские права

Аннотация

Этот документ описывает синтаксис для вложенных параметров согласования S-HTTP в документах HTML. Расширение S-HTTP, описанное в RFC 2660, содержит концептуальное описание заголовков согласования, отражающие потенциальные предпочтения получателя сообщения как криптографическое расширение, которое должно быть применено к сообщению. Документ описывает синтаксис связывания этих параметров согласования с “якорями” HTML.

1. Введение

2. Атрибуты Anchor

Определим три новых атрибута “якорей” (anchor) и передачи форм (form submission):

DN - отличительное имя доверителя (principal), для которого должен шифроваться запрос при разыменовании (dereferencing) “якоря” в url. Это требование не включено в спецификацию, но отказ от его выполнения может привести к тому, что клиент не сможет определить DN и, следовательно, не сможет выполнить шифрование. Имя должно указываться в формате RFC1485 с использованием соглашений SGML.

NONCE - строка произвольного формата (в “кавычках” SGML), которая включается в заголовок SHTTP-Nonce: (после удаления “кавычек” SGML) при разыменовании “якоря”.

CRYPTOPTS - информация о криптографических опциях в соответствии с [SHTTP] (в частности, <cryptopt-list>).

2.1. Элемент CERTS

Определяется новый элемент HTML CERTS, который передает группу сертификатов (не обязательно связанных), обеспечиваемых в качестве дополнительной информации (advisory data). Содержимое этого элемента не предназначено для вывода на экран пользователя. Могут использоваться группы сертификатов для PEM или PKCS-7. Такие сертификаты передаются в документах HTML для удобства получателя, который при отсутствии данных может оказаться неспособен найти сертификаты (цепочки), соответствующие DN, указанному в ссылке (anchor).

Формат элемента должен быть таким же, как для строки заголовка Certificate-Info [SHTTP]; единственное отличие состоит в том, что должен обеспечиваться спецификатор <Cert-Fmt> как атрибут FMT в теге.

Допускается использование множества элементов CERTS; предполагается, что сами элементы CERTS включаются в заголовок (HEAD) документа HTML (чтобы данные из этого элемента не выводились на экран браузерами HTML, которые не поддерживают S-HTTP).

2.2. Элемент CRYPTOPTS

Опции Cryptopts также могут включаться в элемент и указываться в “якоре” по имени. Атрибут NAME задает имя, которым этот элемент может быть указан в атрибуте CRYPTOPTS “якоря”. Имена должны иметь в начале по крайней мере один символ #.

2.3. Пример HTML

Ниже приведен пример криптографических данных, вложенных в “якорь” и содержащих группу сертификатов. Отметим использование синтаксиса SGML для записи данных.

```
<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
Tiq4LnwgTdA8xQX4elJz9QzQobkE3XVOjVAtCFcmiin80RB8AAAMYAAAAAA
AAAAA==
</CERTS>
<A name=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">
Don't read this. </A>
```

3. Вопросы безопасности

Весь документ посвящен вопросам безопасности.

4. Адреса авторов

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

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

5. Литература

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

6. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечивается Internet Society.