

## Безопасность HTML (расширение)

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

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

### Тезисы

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.



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.

## ***Подтверждение***

Финансирование функций RFC Editor обеспечивается Internet Society.