ReferenceMaterials

Reference Materials

This page lists the specifications that are or could be relevant for the design and implementation of HttpClient 4.0.

Protocol

The Hypertext Transfer Protocol (HTTP) is the only protocol directly supported by HttpClient. The current version of the protocol is 1.1, specified by RFC 2616. Version 1.1 maintains backward compatibility with version 1.0, specified by RFC 1945. RFC 1945 is obsoleted by RFC 2616, but still relevant for compatibility.

1. RFC 2616: Hypertext Transfer Protocol – HTTP/1.1
    - RFC 2616 (text)
    - RFC 2616 (HTML)
    - RFC 2616 (PDF)
2. RFC 1945: Hypertext Transfer Protocol – HTTP/1.0 (obsoleted by RFC 2616)
    - RFC 1945 (text)

Cookies

Cookies are the primary means for servers to maintain sessions with clients. They were originally introduced by Netscape, later standardized in RFC 2109, and reworked in RFC 2965. RFC 2109 is obsoleted by RFC 2965, but still relevant for compatibility. Netscape cookies do not conform to the standardized formats, but are relevant as well because they are still used frequently. RFC 2964 documents best practices for using cookies.

1. RFC 2965: HTTP State Management Mechanism
    - RFC 2965 (text)
2. RFC 2964: Use of HTTP State Management
    - RFC 2964 (text)
3. RFC 2109: HTTP State Management Mechanism (obsoleted by RFC 2965)
    - RFC 2109 (text)
4. Netscape Cookies
    - Persistent Client State HTTP Cookies
      It's called a *Preliminary Specification* since it was never finalized. Don't worry, this is the actual specification.

Authentication

Servers can ask clients to authenticate before accessing specific resources or performing restricted operations. The standard authentication mechanisms are Basic and Digest, both specified in RFC 2617. Also frequently used is NTLM, a proprietary protocol for which no complete specification is publicly available.

TLS or SSL with client authentication is **not** handled as part of HTTP. See the section on "Secure Communication" for TLS or SSL.

1. RFC 2617: HTTP Authentication: Basic and Digest Access Authentication
    - RFC 2617 (text)
2. NTLM: NT LAN Manager Authentication
    - http://davenport.sourceforge.net/ntlm.html

Secure Communication

HTTP communication can be encrypted for confidentiality. Netscape developed the original technology called SSL (Secure Sockets Layer) for this purpose. SSL was later enhanced and standardized as TLS (Transport Layer Security) in RFC 2246. TLS is backward compatible with SSL. As the name suggests, encryption is handled on a protocol layer below HTTP. HttpClient does **not** implement TLS nor SSL, it just allows to use them if available.

RFC 2817 specifies the CONNECT method to establish HTTP tunnels through proxies. Such tunnels can then be switched to secure communication. RFC 2818 describes how to use HTTP over TLS connections.

1. RFC 2817: Upgrading to TLS Within HTTP/1.1
    - RFC 2817 (text)
2. RFC 2818: HTTP Over TLS
    - RFC 2818 (text)

Miscellaneous

RFC 1867: Form-based File Upload in HTML

RFC 1867 specifies the MIME type application/x-www-form-urlencoded for sending data from web formulars to HTTP servers. While content encoding itself is not in the scope of HttpClient, posting form data is a requirement. HttpClient needs to provide a mechanism to use an external encoder for generating message bodys with this encoding.

- RFC 1867 (text)

RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax

RFC 2396 specifies the primary format for addressing resources on HTTP servers and elsewhere. HttpClient needs to be able to handle the format used for addressing HTTP servers.

- RFC 2396 (text)

RFC 3143: Known HTTP Proxy/Caching Problems

- RFC 3143 (text)