HTTP State Management Specification

13-DEC-2000

Wireless Application Protocol
WAP-223-HTTPS-20001213-a

A list of errata and updates to this document is available from the WAP Forum™ Web site, http://www.wapforum.org/, in the form of SIN documents, which are subject to revision or removal without notice.

This document is available online in PDF format at http://www.wapforum.org/.

Known problems associated with this document are published at http://www.wapforum.org/.

Comments regarding this document can be submitted to the WAP Forum™ in the manner published at http://www.wapforum.org/.

CONTENTS

1. SCOPE

Wireless Application Protocol (WAP) is a result of continuous work by the WAP Forum to define an industry-wide specification for developing applications that operate over wireless communication networks. The scope of the WAP Forum is to define a set of specifications to be used by service applications for wireless communication devices. The wireless market is growing very quickly and reaching new customers and services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation and fast/flexible service creation, WAP defines a set of protocols in transport, session and application layers. For additional information on the WAP architecture, refer to "*Wireless Application Protocol Architecture Specification"* [WAP].

This specification defines the HTTP state management model for the WAP architecture. The WAP HTTP state management model is an implementation of the HTTP State Management Mechanism, also known as "cookie management", as defined in [RFC2109]. On the World Wide Web, the HTTP State Management mechanism stores state information in a file ("cookie") on the client, as defined in [RFC2109]. The same mechanism can also be used over the WAP protocols, as HTTP headers are used to convey all state and state manipulation information.
Some WAP user agents may have motivation to store and manage cookies locally, as defined in [RFC2109]. This functionality follows precisely the current World Wide Web model, where cookies are typically stored and managed by regular web browsers.

This specification defines an additional mechanism to let an intermediate proxy store and manage cookies on behalf of the WAP client, as an alternative to client-local storage and management. Storing cookies in the network has many advantages. WAP user agents may have a limited storing capacity. When cookies are stored in the proxy, they do not have to be transmitted across the air, for every request/response transaction. In case the user changes device, and cannot move the cookies from the old device to the new one, the user can still access the cookies in the proxy via the new device. On the other hand, storing and managing cookies in the client allows the user to gain the benefit of the same cookies independent of the access point used. This aspect becomes more important in the future in conjunction with WAP gateway roaming architecture. Some users may prefer storing private information in the client, instead of depending on the security of the network. Because both models are complementary, this specification defines a dual approach to WAP HTTP state management, while still maintaining full interoperability between the implementations and RFC2109.

2. DOCUMENT STATUS

This document is available online in the following formats:
- PDF format at http://www.wapforum.org/.

2.1 Copyright Notice

2.2 Errata

Known problems associated with this document are published at http://www.wapforum.org/.

2.3 Comments

Comments regarding this document can be submitted to the WAP Forum in the manner published at http://www.wapforum.org/.

2.4 Document Changes

Change Request	Title	Comments
CR-WAP-223-HTTP-STATE-MGMT-NOKIA-20000913	Backward Compatibility to earlier releases	These changes are as a result of architectural consistency review of the document.
CR-WAP-223-HTTP-STATE-MGMT-NOKIA-20001031	Clarifications from initial Architectural Consistency review	
CR-WAP-223-HTTP-STATE-MGMT-NOKIA-20001213	Editorial changes from closeout architectural consistency review	

2.5 Document History

Document Name	Date of Release
WAP-223-HTTPSM-20000530-d	30-MAY-2000 Draft accepted by WAG
WAP-223-HTTPSM-20000922-d	22-SEP-2000 Draft submitted for proposed
WAP-223-HTTPSM-20001213-d	13-DEC-2000 Reviewed For Architectural Consistency
WAP-223-HTTPSM-20001213-p	24-JAN-2001 Proposed (No changes)
WAP-223-HTTPSM-20001213-a	Approved (No changes)

3. REFERENCES

3.1 Normative References

[RFC2616] "Hypertext Transfer Protocol - HTTP/1.1", R. Fielding, et al., June 1999. URL: http://www.ieft.org/rfc/rfc2616.txt

[RFC2109] "HTTP State Management Mechanism", D. Kristol, et al, February 1997. URL: http://www.ietf.org/rfc/rfc2109.txt

[WAE] "Wireless Application Environment Specification", WAP Forum, 04-November-1999. URL: http://www.wapforum.org/

3.2 Informative References

[RFC2119] "Key words for use in RFC's to Indicate Requirement Levels", S. Bradner, March 1997. URL: http://www.ieft.org/rfc/rfc2119.txt

[WAP] "Wireless Application Protocol Architecture Specification", WAP Forum, 30-April-1998. URL: http://www.wapforum.org/

[WSP] "Wireless Session Protocol", WAP Forum, 30-April-1998. URL: http://www.wapforum.org/

4. DEFINITIONS AND ABBREVIATIONS

4.1 Definitions

The following are terms and conventions used throughout this specification.
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
Client - a device (or application) that initiates a request for a connection with a server.
Cookie Proxy - an intermediate program that acts as a user agent for the purpose of managing cookies and cookie storage on behalf of other user agents.
Origin Server - the server, on which a given resource resides or is to be created, often referred to as a web server or an HTTP server. (also referred to as a "server" in this specification.)
Proxy - an intermediate program that acts as both a server and a client for the purpose of making requests on behalf of other clients ([RFC2616]).
Server - see "origin server".
User - a person, who interacts with a user agent to view, hear or otherwise use a resource.
User Agent - a user agent is any software or device that interprets WML, WMLScript or other content. This may include textual browsers, voice browsers and search engines.
User Agent Session – a session which begins when user agent is activated and ends when it exits.

4.2 Abbreviations

For the purposes of this specification, the following abbreviations apply.

HTTP	Hypertext Transfer Protocol [RFC2616]
RFC	Request For Comments
URI	Universal Resource Identifier
URL	Universal Resource Locator
W3C	World Wide Web Consortium
WAE	Wireless Application Environment [WAE]
WAP	Wireless Application Protocol [WAP]
WSP	Wireless Session Protocol [WSP]

5. OVERVIEW

The HTTP State Management Mechanism is defined in [RFC2109]. In short, RFC2109 defines a means whereby an origin server can request that a small unit of state (a "cookie") is stored in the user agent, and included in subsequent requests to the origin server. A variety of controls are available to the origin server, allowing it to control when the "cookie" is included in subsequent requests, when the "cookie" expires as well as other state management and transport controls. As defined in [RFC2109], the user agent is responsible for cookie management. In this model, the WAP gateway conveys state information between the user agents and the origin servers. It is then the responsibility of the user agent to manage and store the cookies and to offer the user means for control over these functions.

Although RFC2109 puts cookie management in the user agent, it may, in some cases be convenient to take advantage of an architecture, which enables network elements to manage and store cookies. The WAP HTTP State Management Architecture defines the concept of a **Cookie Proxy**. The cookie proxy is an HTTP proxy or proxy equivalent (e.g., WAP Gateway) that manages cookies on behalf of WAP user agents that do not implement the HTTP state function directly. The cookie proxy is responsible for managing and storing cookies on behalf of the user agents, and modifies HTTP requests and responses to and from the user agent to implement this function.

This architecture supports clients with and without local cookie storage, and enables the user agent to control whether proxy cookie storage is enabled. In addition to this, WAP specific HTTP state management headers allow a simple synchronization scheme for user agent and proxy-based cookies. User agents can indicate if they rely on having cookies stored in the Cookie Proxy for a specific user agent session, and Cookie Proxy can notify the user agent if it has problems with their management.

The cookie proxy operation has three stages:

- Enabling or disabling the storage of cookies on the proxy. The user agent controls this function with an HTTP header.
- Origin server request for a cookie to be stored for the duration of the user agent session or for a certain predefined period of time. This is performed via the HTTP `Set-Cookie` header, as specified in [RFC2109].
- Delivery of the cookie to the origin server in subsequent requests. This is performed via the HTTP `Cookie` header, as specified in [RFC2109].

6. HTTP STATE MANAGEMENT HEADERS

6.1 Cookie

`Cookie` header is defined in [RFC2109].

6.2 Set-Cookie

`Set-Cookie` header is defined in [RFC2109].

7. WAP SPECIFIC HTTP STATE MANAGEMENT HEADERS

7.1 X-Wap-Proxy-Cookie

This header is sent in the request from the user agent to indicate whether the Cookie Proxy should store cookies from origin servers or not. `X-Wap-Proxy-Cookie` header is also used to send status information from user agent to the Cookie Proxy.

```
x-wap-proxy-cookie      =   "X-Wap-Proxy-Cookie:" choice
choice                  =   "cache" | "cache-has-state" | "delete" |
                            "none" | "session" | "session-has-state"
```

The choices are introduced briefly as follows:

- When the value is "`cache`" or "`cache-has-state`", the Cookie Proxy caches cookies and sends them to the origin server on behalf of the user agent. Requests and responses between the Cookie Proxy and the origin server include `Cookie` and `Set-Cookie` headers, as they are defined in RFC2109. User agent appends `cache-has-state` value instead of `cache` in case it has received at least one `X-Wap-Proxy-Set-Cookie` header during the ongoing user agent session. This mechanism enables simple method for synchronization between user agents and Cookie Proxy. On account of this information Cookie Proxy can e.g. detect if the user agent session based cookies from the previous usage time should be discarded.

- When the value is "`delete`", the Cookie Proxy does not send any cookies to the origin server or store any received cookies. That is, the proxy acts as a filter ("cookie monster") and deletes all cookies before they are sent to the user agent.

- If the header is not present, or has a value of "`none`", the proxy passes all HTTP cookie headers through between the user agent and the origin server without interception. In this document, a Cookie Proxy executing this function is known as a Pass-Through Cookie Proxy. This is the default condition.

- When the value is "`session`", or "`session-has-state`", Cookie Proxy and user agent functionalities are combined. If Cookie Proxy receives a response containing a `Set-Cookie` header from the origin server, it decides the place for cookie storage according to the presence of the `Max-Age` attribute in the `Set-Cookie` header. This method can be used to separate session-based cookies from long-lived ones. The difference between `session` and `session-has-state` values is similar to the difference between `cache` and `cache-has-state` values, which is described above.

Note that status of the session is bound to the user agent session, which begins when the user agent starts and ends when it exits. Status is not related to a certain cookie-derived session, but it simply tells if the user agent has cookies managed by the Cookie Proxy during a particular user agent session. The user agent session is not related to the concept of session defined in [WSP].

7.2 X-Wap-Proxy-Set-Cookie

This header is sent in the response to the user agent from the Cookie Proxy to indicate that one or more cookies were received in a response from an origin server and stored in the cookie proxy

and/or at least one cookie was sent in the corresponding request. In addition to this, Cookie Proxy uses `X-Wap-Proxy-Set-Cookie` header to report an erroneous status to the user agents.

```
x-wap-proxy-set-cookie   =     "X-Wap-Proxy-Set-Cookie: choice"

choice                   =     "state" | "error"
```

The choices are introduced briefly as follows:

- When value is "`state`", the user-agent is able to detect that a stateful session is in progress. Cookie Proxy sends this value in the response to the user agent when it receives a `Set-Cookie` header from the origin server and chooses to manage the cookie. This header is also sent when the Cookie Proxy has added a `Cookie` header in the related HTTP request.

- When the value is "`error`", Cookie Proxy has detected a mismatch between the status of the user agent and the Cookie Proxy (i.e. Cookie Proxy has lost the cookies during a particular user agent session).

8. WAP GATEWAY RESPONSIBILITIES

The WAP gateway is responsible for delivering state management information between the user agent and the origin server. Header encoding for HTTP state management headers and WAP specific state management headers are defined in [WSP].

9. COOKIE PROXY RESPONSIBILITIES

9.1 Pass Through Cookie Proxy

The Cookie Proxy MUST implement Pass Through Cookie Proxy functionality, i.e. passing the HTTP headers between the user agent and the origin server without interference. If HTTP state management is not implemented in the client user agent, then the actions taken by the Cookie Proxy are undefined in this specification.

9.2 Cookie Management And Storage

The Cookie Proxy MAY be responsible for managing and storing cookies on behalf of user agents. If this functionality is implemented, the `X-Wap-Proxy-Cookie` and `X-Wap-Proxy-Set-Cookie` headers MUST be used for communication between the client and the proxy. The proxy emulates user agent functionality when communicating with origin servers. User agent role in HTTP state management mechanism is defined in RFC2109.

The user agent MAY control the cookie management in the Cookie Proxy with `X-Wap-Proxy-Cookie` header. The Cookie Proxy MUST enforce the following rules when receiving WAP specific HTTP headers from the client (precondition: Cookie Proxy has identified and authenticated the client and chosen to manage cookies on behalf of the user agents)

1. If the choice in `X-Wap-Proxy-Cookie` header equals `cache` or `cache-has-state`, Cookie Proxy MUST cache cookies and send them to the origin server on behalf of the user agent. In addition to this, when Cookie Proxy receives `X-Wap-Proxy-Cookie: cache` header, it MUST discard all the current user agent session -based cookies (i.e. cookies which were sent from the origin server without `Max-Age` –attribute).

2. If the choice in X-Wap-Proxy-Cookie header equals delete, Cookie Proxy MUST NOT send cookies to the origin server or store any received cookies. In addition to this, Cookie Proxy MUST NOT send any received cookies to the client. Cookie Proxy MUST NOT delete any cookies stored prior to receiving the delete header.
3. If the choice in X-Wap-Proxy-Cookie header equals none or the header is missing from the request, Cookie Proxy MUST act as a Pass Through Cookie Proxy.
4. If the choice in X-Wap-Proxy-Cookie header equals session or session-has-state, Cookie Proxy MUST include cookies in the requests to the origin servers. If the Cookie Proxy receives a response containing the Set-Cookie header from the origin server, it MUST decide the place for cookie storage according to the presence of the Max-Age attribute in the Set-Cookie header. If Max-Age attribute is present, cookie MUST be transmitted to the user agent without interception. Otherwise it MUST be stored by the Cookie Proxy until it receives a subsequent X-Wap-Proxy-Cookie: session (or X-Wap-Proxy-Cookie: cache) header from the user agent. Similarly to X-Wap-Proxy-Cookie: cache header, X-Wap-Proxy-Cookie: session effectively indicates that user agent does not have any cookies bound to the current user agent session and thus all stored cookies without Max-Age attribute MUST be discarded.

The Cookie Proxy MUST NOT perform any cookie management, including storage or filtering, without the receipt of an X-Wap-Proxy-Cookie: cache, X-Wap-Proxy-Cookie: cache-has-state, X-Wap-Proxy-Cookie: session or X-Wap-Proxy-Cookie: session-has-state header from the user agent, indicating that cookie management is desired.

The Cookie Proxy MUST be prepared to receive Cookie headers from the user agent, regardless of the presence of an X-Wap-Proxy-Cookie header. If this situation occurs, the Cookie Proxy MUST transmit the state present in the Cookie header to the origin server, with the following criteria:

1. If a cookie proxy receives both Cookie and X-Wap-Proxy-Cookie: cache/cache-has-state or X-Wap-Proxy-Cookie: session/session-has-state headers, the Cookie Proxy may append other cookies to the Cookie header prior to performing the subsequent HTTP request. In the case where a user agent and a Cookie Proxy have an identical cookie to send, i.e. both cookies have identical values for path, domain and NAME attributes, the cookie MUST be delivered to the origin server as it is specified by the user agent. Cookies MUST be ordered in the Cookie header as specified in [RFC2109].
2. If cookie proxy receives both Cookie and X-Wap-Proxy-Cookie: delete or X-Wap-Proxy-Cookie: none headers, it MUST deliver the cookie header to the origin server without interception.

Cookie Proxy MUST include X-Wap-Proxy-Set-Cookie: state header in the response to the client, if it has received a cookie in the response from the origin server and chosen to manage it or it has sent a Cookie header in the associated HTTP request. . This header MUST NOT be sent if neither of the Cookie and Set-Cookie headers was present in the HTTP request and response, or if the cookie proxy has not cached any cookie information.

Cookie Proxy MUST include X-Wap-Proxy-Set-Cookie: error header in the response if user agent sends status information which is conflicting with the status recorded by the Cookie Proxy. This will happen when a user agent sends a request with X-Wap-Proxy-Cookie: cache-has-state or X-Wap-Proxy-Cookie: session-has-state header, but the Cookie Proxy does not have any cookies in storage for this particular user agent.

Cookie Proxy MUST NOT store the received cookie, if `Set-Cookie` header includes `secure` attribute. If `secure` attribute is present, Cookie Proxy MUST deliver the cookie to the client without interception. This attribute MAY be used by content authors to indicate that a specific cookie contains private or confidential information, and that the preferred storage is in the client. If a cookie proxy receives an `X-Wap-Proxy-Cookie` header from a client and chooses to manage and store cookies on its behalf, it MUST remove the `X-Wap-Proxy-Cookie` header from the request and thus prevent it from going further to the network. If Cookie Proxy chooses not to manage cookies on behalf of the client, it MUST let the headers pass without interception.

9.3 Associating Cookie Storage With Clients

The Cookie Proxy MUST associate cookies with a single client and prevent another client from gaining access to the cookies. This may be achieved by associating the cookies with an authenticated client identifier. Content authors should be advised that different user agents located in the same client may use the same Cookie Proxy facilities and the same cookie storage.

The Cookie Proxy MUST NOT provide cookie proxy facilities to anonymous clients.

9.4 Managing Proxy Cookies

The Cookie Proxy SHOULD provide a Web application to let the user browse and control the stored cookies.

10. USER AGENT RESPONSIBILITIES

10.1 HTTP State Management

The user agent MUST implement HTTP State Management, as specified in [RFC2109]. User agents with non-conforming implementations (i.e. no support) have undefined semantics. WAP user agents MUST be able to save and manage at least four cookies, with a maximum size of 125 bytes each (size includes fully-qualified host name, expiration date, and cookie data).

10.2 Cookie Proxy Management

Support for use of Cookie Proxy functionality in the user agent is optional. User agent MAY include WAP Specific HTTP State Management Headers in requests to utilize Cookie Proxy facilities. If Cookie Proxy functionality is supported, end-user MUST have an opportunity to elect to use either cookie proxy facilities or their own local cookie management or both.

User agent MUST send `X-Wap-Proxy-Cookie: cache-has-state` header instead of `X-Wap-Proxy-Cookie: cache` and `X-Wap-Proxy-Cookie: session-has-state` header instead of `X-Wap-Proxy-Cookie: session` in case it has received at least one `X-Wap-Proxy-Set-Cookie` header during the ongoing user agent session. When user agent receives `X-Wap-Proxy-Set-Cookie: error` header, it MAY notify the user that inconsistent service behavior might occur. WAP user agents MUST be prepared to receive `Set-Cookie` HTTP headers even when they have requested Cookie Proxy functionality alone, and must act in accordance with [RFC2109] in this situation (e.g., the user agent should make a best effort attempt to manage the cookie (See section 10.2)).

11. STATIC CONFORMANCE REQUIREMENTS

These static conformance requirements define a minimum set of features that must be implemented to support the WAP HTTP State Management mechanism. A feature can be optional (O), mandatory (M) or conditional (C (<condition>)). If optional/conditional features have labels (O.<n> or C.<n>), support of at least one of the group of options labeled by the same number is required.

11.1 User Agent Features

Item	Functionality	Reference	Status	Requirement
HSM_C001	User agent support for HTTP State Management Mechanism	10.1	M	
HSM_C002	User agent support for at least four cookies of at least 125 bytes total storage space.	10.1	M	
HSM_C003	User agent support for more than 500 bytes of cookie storage space	10.1	O	
HSM_C004	User agent support for use of Cookie Proxy functionality	10.2	O	
HSM_C005	User agent support for WAP specific HTTP State management headers	10.2	C:HSM_C004	

11.2 Cookie Proxy Features

Item	Functionality	Reference	Status	Requirement
HSM_S001	Cookie Proxy support for passing of HTTP headers between the user agent and the origin server without interference.	9.1	M	
HSM_S002	Cookie Proxy support for Cookie Management and Storage functionality.	9.2	O	
HSM_S003	Cookie Proxy support for user agent role in HTTP State Management Mechanism.	9.2	C:HSM_S002	
HSM_S004	Cookie Proxy support for WAP specific HTTP State Management headers and mechanisms.	9.2	C:HSM_S002	
HSM_S005	Cookie Proxy does not store the cookie if origin server includes `secure` attribute in `Set-Cookie` header.	9.2	C:HSM_S002	
HSM_S006	Cookie Proxy associates HTTP state with a particular client, and does not provide cookie management or storage for anonymous clients.	9.3	C:HSM_S002	
HSM_S007	Cookie Proxy support for WAP HTTP State Management user interface	9.4	O	