Specification

Browser Request Protocol Specification

Document number: ST17455121

Revision: A

Contents

Document number: ST17455121
Revision: A

1 Introduction

This protocol specification describes the protocol between the Wireless Internet Gateway (WIG) Server and the Content Provider (CP). The WIG Server acts as a client to the CP.

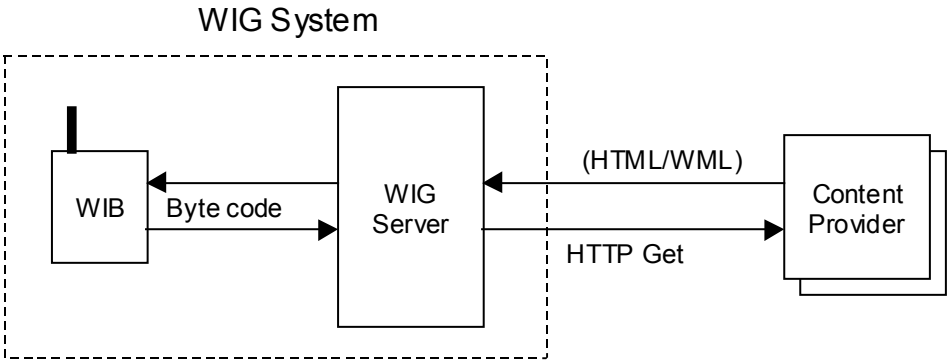

Figure 1. WIG system-Content Provider.

Document number: ST17455121
Revision: A

2 References

Ref.	Title	Document No.
[1]	Hypertext Transfer Protocol HTTP/1.1, RFC 2068, Version 1997-01, http://www.cis.ohio-state.edu/htbin/rfc/rfc2068.html	
[2]	WML Specification – Wireless Internet Gateway	ST17455119
[3]	GSM 11.14 version 7.3.1, Release 1998, ETSI	
[4]	RFC 2109, HTTP State Management Mechanism	

3 Protocol description

The protocols between the request module of the WIG Server and the CP are the standard Internet protocols HTTP and TCP/IP. Only the HTTP Get method of the HTTP protocol is supported, see reference [1].

The HTTP protocol is a request/response protocol. A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a connection with a server. The server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity metainformation, and possible entity-body content.

3.1 Technical Overview

The Wireless Internet Browser (WIB) makes an URL request. The WIG Server receives the request and translates it into an HTTP Get request. The mobile phone number, MSISDN is attached to the HTTP Get request at the end of the form data set (query string). Example:

```
www.across.se?first+name=Anders&last+name=Jansson&MSISDN=070341032
1
```

The Content Provider receives the HTTP Get request and an HTTP response is returned including an HTML/WML document.

The WIG server parses the HTTP response and compresses the HTML/WML see reference [2], document into byte code. The WIB receives the sequence of commands in byte code from the WIG server and runs these commands. The WIB will use SIM Application Toolkit, see reference [3], for user interactive commands.

To handle secure browser request transaction between the WIG Server and the Content Provider the secure socket layer (SSL) may be used.

3.2 HTTP Header

The HTTP header of the GET request contains the following fields:

- Accept
- User Agent
- Connection

- Host
- Cookie

3.2.1 User Agent

The user agent field contains information about the user agent originating the request. In the WIG Server this field is used to communicate the version of the WIG Browser on the SIM card, e.g “User Agent: WIG Browser 1.0”.

3.2.2 Accept Header

The accept header field is used to specify certain media types which are acceptable for the response. In the WIG Server the following values are used.

Accept: text/*
Accept-Charset: iso-8859-1, UTF-8
Accept-Encoding: identity

3.2.3 Cookie

Cookies are supported by the WIG Server and handled according to RFC 2109, HTTP State Management Mechanism, see Reference [4]. If the response contains a cookie the host and path attribute will be checked to see if the cookie will be accepted. The cookie is rejected if any of the following is true.

- The value for the Path attribute is not a prefix of the request-URI.
- The value for the Domain attribute contains no embedded dots or does not start with a dot.
- The value for the request-host does not domain-match the Domain attribute.
- The request-host is a FQDN (not IP address) and has the form HD, where D is the value of the Domain attribute, and H is a string that contains one or more dots.

If the cookie is not rejected it will be stored in the database and included in subsequent requests. The cookie will be added to the request if the following is true.

- The origin server’s fully-qualified host name must domain-match the Domain attribute of the cookie.
- The Path attribute of the cookie must match a prefix of the request-URI.

- Cookies that have expired will be discarded and thus not forwarded to an origin server.

Only the name-value pair attribute are included in the Cookie sent in the request. No other attributes are included at the moment.

The cookies are valid as long as the max-age attribute specifies. If no max-age attribute is included in the cookie a default value of one hour is used. It is configurable if the cookies are removed from the database manually by a script or automatically when the max-age has been reached.