



**ПЕРВЫЙ  
ЗАМЕСТИТЕЛЬ МИНИСТРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПО СВЯЗИ И ИНФОРМАТИЗАЦИИ**

ул. Тверская, 7, Москва, 125375

Справочная: 771-81-00  
по документам: 771-81-21

Факс: 771-87-18

Телерайп: 114158 MSRF RU

E-mail: office@minsvyaz.ru

Сайт: www.minsvyaz.ru

Руководителям структурных  
подразделений  
Минсвязи России

Руководителям организаций

10.07.2003 № БА-ПЗ-4050

На № \_\_\_\_\_

**О введении в действие Дополнения №1 к руководящему документу  
отрасли РД45.201-2001**

Министерством Российской Федерации по связи и информатизации утверждено и вводится в действие с 4 июля 2003 года Дополнение №1 к руководящему документу отрасли РД45.201-2001 «Шлюзы WAP для систем подвижной радиосвязи. Общие технические требования».

Разработчиком данного документа является ФГУП ЛОНИИС. Телефон для справок: (812) 389 31 86.

Издание и распространение руководящего документа отрасли будет осуществлять Центр научно-технической информации «ИНФОРМСВЯЗЬ» (105275, г.Москва, ул. Уткина, д.44). Телефон для справок (факс): 273 30 60, 273 37 80.

Б.Д.Антонюк

## Дополнение №1 руководящего документа отрасли

# **ШЛЮЗЫ ПРОТОКОЛА БЕСПРОВОДНЫХ ПРИЛОЖЕНИЙ (WAP) ДЛЯ СИСТЕМ ПОДВИЖНОЙ РАДИОСВЯЗИ**

## **Общие технические требования**

## Дата введения

В РД 45.201-2001 добавить § 6.

### **6. Технические требования к шлюзам WAP, использующим архитектуру протокола WAP 2.0**

#### **6.1 Архитектура протокола WAP 2.0**

Протокол WAP версии 2.0 использует шлюзы/фильтры (проxy), обеспечивающие:

а) трансформацию протоколов TCP и HTTP в профили указанных протоколов для беспроводной связи TCP\* [a1] и HTTP\* [a2] (пример архитектуры протокола – см.рис.4);

б) трансформацию протокола TCP в TCP\* [a1] и обеспечения туннеля с использованием протокола транспортного уровня TLS [a3, a17] в режиме с установлением соединения (пример архитектуры протокола – см.рис.5);

в) трансляцию пакетов IP между проводным и беспроводным интерфейсом с использованием протокола безопасности на уровне доставки информации [a4] (пример архитектуры протокола – см.рис.6).

Абонентское устройство  
с поддержкой WAP

Шлюз/фильтр WAP

Web-сервер

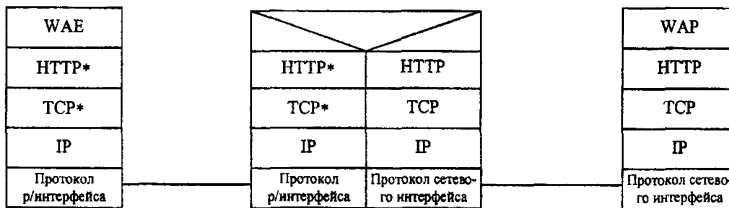


Рис.4

Абонентское устройство  
с поддержкой WAP

Шлюз/фильтр WAP

Web-сервер

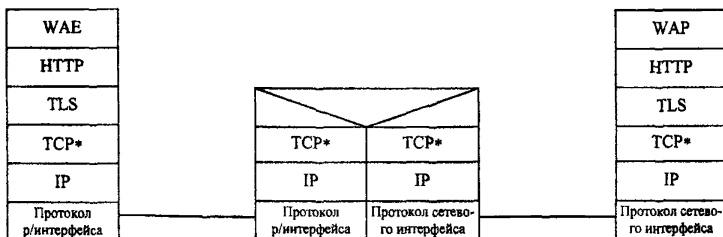


Рис.5

Абонентское устройство  
с поддержкой WAP

Шлюз/фильтр WAP

Web-сервер

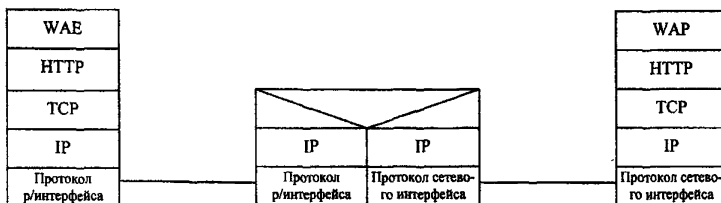


Рис.6

## 6.2 Технические требования к функциональным характеристикам

6.2.1 Требования к функциональным характеристикам шлюзов WAP, в отношении которых применяется декларирование, должны соответствовать технической спецификации WAP – 262 – Class Conformance Requirements – Version 17-May-2002 [a5]. Объем требований приведен в таблице 6.1.

Детальная спецификация требований, подлежащих декларированию фирмой-изготовителем, приведена в пп.6.2.2-6.2.19.

6.2.2 Требования к прикладному уровню WAP – WAE для WAP версии 2.0 должны соответствовать технической спецификации WAP-236 Wireless Application Environment Specification", Version 2 [a6]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.2. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.2.

Таблица 6.1

Функция протокола WAP версии 2.0	Обязательность наличия
1. Архитектура протокола: согласно п.4 рис.2-3 без поддержки WTLS согласно п.4 рис.2-3 с поддержкой WTLS согласно п.6.1 а) рис.4 согласно п.6.1 б) и/или в) рис.5, 6	Как минимум одна из перечисленных опций
2. Уровень WAE	Опция
3. Услуга push	Опция
4. Услуга передачи мультимедийных сообщений с использованием WAP	Опция
5. Услуга минимизации взаимодействия с пользователем (provisioning)	Опция
6. Прикладные услуги беспроводной телефонии	Опция
7. Синхронизация данных	Опция

Таблица 6.2

Условное обозначение	Соответствие [a6]	Наименование функции	Обязательность поддержки
1	2	3	4
WAESpec-WMLS-S-S001	п.6.4 [a6]	Возможность трансформации языка разметки WMLScript в октеты	О
WAESpec-WMLS-S-S002	п.6.4 [a6]	Уведомление об ошибках компиляции с использованием статус-кода HTTP 502 (Bad Gateway)	Опц.
WAESpec-MUL-S-S001	п.6.9.5 [a6]	Возможность преобразования многочастевых данных из формата application/vnd.wap.multipart.form-data в multipart/form-data	О
WAESpec-MUL-S-S002	п.6.9.2 [a6]	Возможность преобразования многочастевых данных из формата application/vnd.wap.multipart.mixed в multipart/mixed	Опц.
WAESpec-MUL-S-S003	п.6.9.3 [a6]	Возможность преобразования многочастевых данных из формата application/vnd.wap.multipart.related в multipart/related	Опц.
WAESpec-MUL-S-S004	п.6.9.4 [a6]	Возможность преобразования многочастевых данных из формата application/vnd.wap.multipart.alternative в multipart/alternative	Опц.
WAESpec-HTS-S-S001	п.7.1.1 [a6]	Поддержка услуги передачи гипермедиа (одна из опций WAESpec-HTS-S002 или WAESpec-HTS-S003)	О
WAESpec-HTS-S-S002	п.7.1.1 [a6]	Поддержка WSP	Опц. (требуется поддержка обязательных функций согласно п.6.2.4)
WAESpec-HTS-S-S003	п.7.1.1 [a6]	Поддержка W-HTTP	Опц. (требуется поддержка обязательных функций согласно п.6.2.3)
WAESpec-HTS-S-S004	п.7.1.4 [a6]	Обработка заголовка пользователя примитивом Connect	Опц.
WAESpec-HTS-S-S005	п.7.1.4 [a6]	Обработка заголовка пользователя примитивом Resume	Опц.
WAESpec-URI-S-S001	п.7.2 [a6]	Поддержка универсального идентификатора ресурса (URI) [a9] длиной не менее чем 1024 октета	О

Продолжение таблицы 6.2

1	2	3	4
WAESpec-URI-S-S002	п.7.2.1 [a6]	Поддержка схемы URI для HTTP	О
WAESpec-URI-S-S003	п.7.2.2 [a6]	Поддержка схемы URI для HTTPS (одна из опций WAESpec-URI-S004, WAESpec-URI-S005 или WAESpec-URI-S006)	О
WAESpec-URI-S-S004	п.7.2.2 [a6], [a10]	Поддержка схемы URI для HTTPS с использованием протокола W-HTTP	Опц. (требуется поддержка обязательных функций согласно п.6.2.8)
WAESpec-URI-S-S005	п.7.2.2 [a6], [a11]	Поддержка схемы URI для HTTPS с использованием протокола WSP	Опц. (требуется поддержка обязательных функций согласно п.6.2.6)
WAESpec-URI-S-S006	п.7.2.2 [a6]	Уведомление об ошибке (HTTP 502 (Bad Gateway) в случае, когда схема URI (WAESpec-URI-S004 и WAESpec-URI-S005) не поддерживается	О
WAESpec-I18N-S-S001	п.7.4.1 [a6]	Возможность преобразования символьной кодировки в случае, когда исходная символьная кодировка не поддерживается	Опц.
WAESpec-I18N-S-S002	п.7.4.1 [a6]	Поддержка UTF-8	О
WAESpec-I18N-S-S003	п.7.4.1 [a6]	Поддержка UTF-16	О
WAESpec-I18N-S-S004	п.7.4.1 [a6], [a12]	Уведомление пользователя об ошибках в XML-документе, в т.ч. о неизвестных символах	О
WAESpec-UAC-S-S001	п.7.5.1 [a6] п.14.1 [a7] п.7.5.1 [a13]	Поддержка поля заголовка запроса Ассерпт при обмене с программой-агентом пользователя	О
WAESpec-UAC-S-S002	п.7.5.1 [a6] п.14.2 [a7] п.7.5.1 [a13]	Поддержка поля заголовка запроса Ассерпт-Charset при обмене с программой-агентом пользователя	О
WAESpec-UAC-S-S003	п.7.5.1 [a6] п.14.3 [a7] п.7.5.1 [a13]	Поддержка поля заголовка запроса Ассерпт-Encoding при обмене с программой-агентом пользователя	О
WAESpec-UAC-S-S004	п.7.5.1 [a6] п.14.4 [a7] п.7.5.1 [a13]	Поддержка поля заголовка запроса Ассерпт-Language при обмене с программой-агентом пользователя	О
WAESpec-UAC-S-S005	п.7.5.1 [a6] п.12.1 [a7]	Обработка полей заголовка запроса при обмене с программой-агентом пользователя	Опц.
WAESpec-UAC-S-S006	п.7.5.1 [a6]	Учёт установок программы-агента пользователя и трансформация языка разметки WML1 (см.п.5.1.3) в WML2 [a14] в случае, когда использование последнего предпочтительнее	Опц.
WAESpec-UAC-S-S007	п.7.5.1 [a6]	Предотвращение передачи контента в случае если его формат не поддерживается программой-агентом пользователя	Опц.

Продолжение таблицы 6.2

1	2	3	4
WAESpec-UAC-S-S008	п.7.5.1 [a6]	Предотвращение избыточного преобразования способа кодирования сообщения	О
WAESpec-SEC-S-S001	п.7.10.3 [a6]	Поддержка возможности компиляции содержания с использованием WMLScript Crypto (см.п.5.1.12)	О

Примечание: Опц – опциональность поддержки, О – обязательность поддержки.

6.2.3 Требования к поддержке функций модифицированного протокола передачи гипертекстов HTTP должны соответствовать технической спецификации WAP-229 – HTTP-20010329-a. Wireless Profiled HTTP [a2]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.3.

Таблица 6.3

Условное обозначение	Соответствие [a2]	Наименование функции	Обязательность поддержки
HTTP-S-S001	п.5.2.2 [a2]	Поддержка реализации HTTP Server	О
HTTP-S-C001	п.5.2.1 [a2]	Поддержка реализации HTTP Client	Опц.
HTTP-S-C002	п.5.2.1 [a2], п.9.3 RFC2616 [a7]	Поддержка метода GET	О – при наличии HTTP-S-C001
HTTP-S-C003	п.5.2.1 [a2], п.9.5 RFC2616 [a7]	Поддержка метода POST	О – при наличии HTTP-S-C001
HTTP-S-C004	п.5.2.1 [a2], п.9.2 RFC2616 [a7]	Поддержка метода OPTIONS	О – при наличии HTTP-S-C001
HTTP-S-S002	п.5.2.2 [a2], п.9.3 RFC2616 [a7]	Поддержка метода GET	О – при наличии HTTP-S-S001
HTTP-S-S003	п.5.2.2 [a2], п.9.5 RFC2616 [a7]	Поддержка метода POST	О – при наличии HTTP-S-S001
HTTP-S-S004	п.5.2.2 [a2], п.9.4 RFC2616 [a7]	Поддержка метода HEAD	О – при наличии HTTP-S-S001
HTTP-S-S005	п.5.2.2 [a2], п.9.2 RFC2616 [a7]	Поддержка метода OPTIONS	О – при наличии HTTP-S-S001
HTTP-S-S006	пп.5.2.2, 5.4.1 [a2], п.5 RFC2817 [a8]	Поддержка метода CONNECT	О – при наличии HTTP-S-S001
HTTP-S-S007	п.5.3.1 [a2], п.3.5 RFC2616 [a7]	Поддержка метода сокращённого кодирования (deflate) контента	О – при наличии HTTP-S-S001

6.2.4 Требования к поддержке функций протокола сеансового уровня (WSP) для WAP версии 2.0 должны соответствовать технической спецификации WAP-230 – WSP-20010705-a. Wireless Session Protocol Specification [a13]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.4. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.13.

Таблица 6.4

Условное обозначение	Соответствие [a13]	Наименование функции	Обязательность поддержки
1	2	3	4
WSP-C-001	пп.6-8 [a13]	Режим передачи (WSP-CL-C-001 или WSP-CO-C-001)	О
WSP-CL-S-001	пп.6-8 [a13]	Режим без установления соединения	Опц.

Продолжение таблицы 6.4

1	2	3	4
WSP-CO-S-001	пп.6-8 [a13]	Режим с установлением соединения	Опц.
WSP-CO-S-002	пп.6.3.3.1, 6.3.4, 7.1.2.1, 7.1.5, 7.1.6.4, 8.2.2.1 [a13]	Установление соединения сеансового уровня. Блок данных протокола Connect PDU	О
WSP-CO-S-003	пп. 7.1.2.1, 7.1.5, 7.1.6.4, 8.2.2.2 [a13]	Установление соединения сеансового уровня. Блок данных протокола Connect Reply PDU	О
WSP-CO-S-004	пп. 7.1.2.1, 7.1.5, 7.1.6.4, 8.2.2.3 [a13]	Установление соединения сеансового уровня. Блок данных протокола Redirect PDU	Опц.
WSP-CO-S-005	пп. 6.3.2, 6.3.3.1, 6.3.3.4, 7.1.5, 7.1.6.4, 8.2.2.1, 8.3 [a13]	Согласование возможностей сервера и клиента. Блок данных протокола Capability Negotiation – Connect PDU	О
WSP-CO-S-006	пп. 7.1.5, 7.1.6.4, 8.2.2.2, 8.3 [a13]	Согласование возможностей сервера и клиента. Блок данных протокола Capability Negotiation – Connect Reply PDU	О
WSP-CO-S-007	пп.6.3.3.2, 7.1.2.1, 7.1.5, 7.1.6.4, 8.2.2.4 [a13]	Разъединение соединения сеансового уровня. Блок данных протокола Disconnect PDU	О
WSP-CO-S-008	пп.6.3.3.3, 7.1.2.2, 7.1.5, 7.1.6.4, 8.2.5.1 [a13]	Приостановление соединения сеансового уровня. Блок данных протокола Suspend PDU	Опц.
WSP-CO-S-009	пп.6.3.3.4, 7.1.2.2, 7.1.5, 7.1.6.4, 8.2.5.2 [a13]	Восстановление соединения сеансового уровня. Блок данных протокола Resume PDU	Опц.
WSP-CO-S-010	пп.6.3.3.9, 7.1.2.4, 8.2.4.1 [a13]	Соединение в режиме push. Блок данных протокола Push PDU	Опц.
WSP-CO-S-011	пп.6.3.3.10, 6.3.3.11, 6.3.4, 7.1.2.5, 7.1.5, 7.1.6.6, 8.2.4.1 [a13]	Соединение в режиме confirmed push. Блок данных протокола Confirmed Push PDU	Опц.
WSP-CO-S-012	пп.6.3.3.7, 6.3.3.10, 7.1.6.5, 7.1.6.6, 8.2.4.2 [a13]	Использование заголовков подтверждения.	Опц.
WSP-CO-S-013	пп.6.3.3.2, 8.3.2.4 [a13]	Использование расширенных методов запроса клиента на сервер.	Опц.
WSP-CO-S-014	пп.6.3.2.2, 8.4 Табл.39 [a13]	Кодирование заголовка. Параметры, устанавливаемые по умолчанию.	О
WSP-CO-S-015	пп.6.3.2.2, 8.3.2.5 [a13]	Кодирование заголовка. Расширенный формат.	Опц.
WSP-CO-S-016	пп.6.3.2.2, 8.3.2.5 [a13]	Перечень альтернативных адресов для отправителя информации	Опц.
WSP-CO-S-017	пп.6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.1 [a13]	Метод GET. Блок данных протокола Get PDU	О
WSP-CO-S-018	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод GET. Блок данных протокола Reply PDU	О

Продолжение таблицы 6.4

1	2	3	4
WSP-CO-S-019	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.2, 8.2.3.4 [a13]	Метод GET. Блок данных протокола Data Fragment PDU	Опц.
WSP-CO-S-020	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.2 [a13]	Метод POST. Блок данных протокола Post PDU	О
WSP-CO-S-021	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод POST. Блок данных протокола Reply PDU	О
WSP-CO-S-022	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.2, 8.2.3.4 [a13]	Метод POST. Блок данных протокола Data Fragment PDU	Опц.
WSP-CO-S-023	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.1 [a13]	Метод DELETE. Блок данных протокола Get PDU	Опц.
WSP-CO-S-024	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод DELETE. Блок данных протокола Reply PDU	Опц.
WSP-CO-S-025	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.1 [a13]	Метод HEAD. Блок данных протокола Get PDU	Опц.
WSP-CO-S-026	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод HEAD. Блок данных протокола Reply PDU	Опц.
WSP-CO-S-027	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.1 [a13]	Метод OPTIONS. Блок данных протокола Get PDU	Опц.
WSP-CO-S-028	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод OPTIONS. Блок данных протокола Reply PDU	Опц.
WSP-CO-S-029	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.1 [a13]	Метод TRACE. Блок данных протокола Get PDU	Опц.
WSP-CO-S-030	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод TRACE. Блок данных протокола Reply PDU	Опц.
WSP-CO-S-031	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.2 [a13]	Метод PUT. Блок данных протокола Post PDU	Опц.



Продолжение таблицы 6.4

1	2	3	4
WSP-CO-S-032	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Метод PUT. Блок данных протокола Reply PDU	Опц.
WSP-CO-S-033	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.2, 8.2.3.4 [a13]	Метод PUT. Блок данных протокола Data Fragment PDU	Опц.
WSP-CO-S-034	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.2 [a13]	Многочастевые данные. Блок данных протокола Post PDU	Опц.
WSP-CO-S-035	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.5, 8.2.3.3 [a13]	Многочастевые данные. Блок данных протокола Reply PDU	Опц.
WSP-CO-S-036	6.3.3.6, 6.3.3.7, 6.3.3.8, 6.3.4, 7.1.2.3, 7.1.5, 7.1.6.2, 8.2.3.4 [a13]	Многочастевые данные. Блок данных протокола Data Fragment PDU	Опц.
WSP-CO-S-037	8.4.1, 8.4.2.70 [a13]	Версия кодирования	О
м без протокола по п.6.2.7			
WSP-CL-S-002	6.4.2.3, 6.3.4, 7.2, 8.2.4.1 [a13]	Соединение в режиме push. Блок данных протокола Push PDU	Опц.
WSP-CL-S-003	8.4 (табл.39) [a13]	Кодирование заголовка. Параметры, устанавливаемые по умолчанию.	О
WSP-CL-S-004	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.1 [a13]	Метод GET. Блок данных протокола Get PDU	О
WSP-CL-S-005	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод GET. Блок данных протокола Reply PDU	О
WSP-CL-S-006	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.2 [a13]	Метод POST. Блок данных протокола Post PDU	О
WSP-CL-S-007	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод POST. Блок данных протокола Reply PDU	О
WSP-CL-S-008	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.1 [a13]	Метод DELETE. Блок данных протокола Get PDU	Опц.
WSP-CL-S-009	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод DELETE. Блок данных протокола Reply PDU	Опц.
WSP-CL-S-010	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.1 [a13]	Метод HEAD. Блок данных протокола Get PDU	Опц.
WSP-CL-S-011	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод HEAD. Блок данных протокола Reply PDU	Опц.
WSP-CL-S-012	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.1 [a13]	Метод OPTIONS. Блок данных протокола Get PDU	Опц.
WSP-CL-S-013	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод OPTIONS. Блок данных протокола Reply PDU	Опц.
WSP-CL-S-014	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.1 [a13]	Метод TRACE. Блок данных протокола Get PDU	Опц.
WSP-CL-S-015	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод TRACE. Блок данных протокола Reply PDU	Опц.
WSP-CL-S-016	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.2 [a13]	Метод PUT. Блок данных протокола Post PDU	Опц.
WSP-CL-S-017	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Метод PUT. Блок данных протокола Reply PDU	Опц.

Продолжение таблицы 6.4

1	2	3	4
WSP-CL-S-018	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.2 [a13]	Многочастевые данные. Блок данных протокола Post PDU	Опц.
WSP-CL-S-019	6.4.2.1, 6.4.2.2, 6.4.3, 7.2, 8.2.3.3 [a13]	Многочастевые данные. Блок данных протокола Reply PDU	Опц.
WSP-CL-S-020	8.4.1, 8.4.2.70 [a13]	Версия кодирования	О

6.2.5 Требования к поддержке функций уровня транзакций (WTP) для WAP версии 2.0 должны соответствовать технической спецификации WAP-224 – WTP-20010710-a. Wireless Transaction Protocol [a15]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.5. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.14.

Таблица 6.5

Условное обозначение	Соответствие [a15]	Наименование функции	Обязательность поддержки
1	2	3	4
WTP-S-001	п.6.1.3 [a15]	Транзакция класса 0 – действия инициатора	О
WTP-S-002	п.6.1.3 [a15]	Транзакция класса 0 – действия ответчика	О
WTP-S-003	п.6.2.4 [a15]	Транзакция класса 1 – действия инициатора	О (при поддержке WTP-S-022, 015)
WTP-S-004	п.6.2.4 [a15]	Транзакция класса 1 – действия ответчика	О (при поддержке WTP-S-022)
WTP-S-005	п.6.3.4 [a15]	Транзакция класса 2 – действия инициатора	Опц. (при поддержке WTP-S-022, 015)
WTP-S-006	п.6.3.4 [a15]	Транзакция класса 2 – действия ответчика	О (при поддержке WTP-S-022)
WTP-S-007	п.7.3 [a15]	Подтверждение получения абонентом сообщений от сервера	Опц.
WTP-S-008	пп.4.1, 7.5 [a15]	Процедура передачи нескольких блоков данных протокола WTP в одной датаграмме – concatenation	Опц.
WTP-S-009	п.7.5 [a15]	Процедура извлечения нескольких блоков данных протокола WTP из одной датаграммы – separation	О
WTP-S-010	п.7.2 [a15]	Повторная передача пакетов вплоть до получения их подтверждения	Опц.
WTP-S-011	пп.4.6, 7.7, 7.12 [a15]	Прерывание невыполненных транзакций	Опц.
WTP-S-012	п.7.12 [a15]	Прерывание транзакций в случае возникновения неисправимых ошибок	Опц. (при поддержке WTP-S-011)
WTP-S-013	пп.7.4, 7.12 [a15]	Помещение информации в последнее подтверждение транзакции	Опц. (при поддержке WTP-S-018)
WTP-S-014	п.7.6 [a15]	Асинхронная обработка транзакций	Опц.
WTP-S-015	п.7.1.5.2 [a15]	Проверка идентификатора транзакций - действия инициатора	Опц.

Продолжение таблицы 6.5

1	2	3	4
WTP-S-016	пп.7.1.5.2, 7.8.1 [a15]	Проверка идентификатора транзакций - действия ответчика	Опц.
WTP-S-017	пп.7.10, 8.4.2 [a15]	Заголовок информации транспортного уровня (TPI); TPI = Error	Опц.
WTP-S-018	пп.7.10, 8.4.3 [a15]	TPI = Info	Опц.
WTP-S-019	пп.7.10, 8.4.4 [a15]	TPI = Option	Опц.
WTP-S-020	пп.7.10, 8.4.5 [a15]	TPI = PSN	Опц.
WTP-S-021	п.7.14 [a15]	Сегментация и десегментация с выборочной повторной передачей	Опц. (при поддержке WTP-S-020)
WTP-S-022	п.7 [a15]	Режим передачи	Опц. (при поддержке WTP-S-007, 010, 011 и 012)
WTP-S-023	п.7.15 [a15]	Расширенная сегментация и десегментация с выборочной повторной передачей	Опц. (при поддержке WTP-S-019, 020, 024 и 025)
WTP-S-024	пп.7.15.2, 8.4.7 [a15]	TPI = Frame Boundary	Опц.
WTP-S-025	пп.7.15.2, 8.4.8 [a15]	TPI = SDU Boundary	Опц.
WTP-S-026	пп.7.15.2, 7.15.3 [a15]	Поддержка режима со скользящим окном и расширенной сегментацией и десегментацией	Опц.

6.2.6 Требования к поддержке функций уровня безопасности (WTLS) для WAP версии 2.0 должны соответствовать технической спецификации WAP-261 – WTLS-20010406-a. Wireless Transport Layer Security [a11]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.6. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.15.

Таблица 6.6

Условное обозначение	Соответствие [a11]	Наименование функции	Обязательность поддержки
1	2	3	4
WTLS-S-001	п.10.3 [a11]	Протокол full handshake	О
WTLS-S-002	п.10.3 [a11]	Протокол abbreviated handshake	О
WTLS-S-003	п.10.3 [a11]	Протокол optimised public key handshake	Опц.
WTLS-S-004	п.11.1.4 [a11]	Восстановление соединения без повторного расчёта параметра master secret	Опц.
WTLS-S-005	п.10.4 [a11]	Последовательное соединение записей для сообщений handshake	О
WTLS-S-006	п.10.4 [a11]	Передача сообщений handshake с использованием датаграмм	О
WTLS-S-007	п.10.5.1 [a11]	Передача сообщения hello_request	Опц.
WTLS-S-010	п.9.2.3.1 [a11]	Явная порядковая нумерация	О
WTLS-S-011	п.9.2.3.1 [a11]	Неявная порядковая нумерация	Опц.
WTLS-S-012	п.9.2.3.1 [a11]	Удаление вторично принятых записей	О
WTLS-S-013	доп.В3 [a11]	Обновление ключей шифрования	О

Продолжение таблицы 6.6

1	2	3	4
WTLS-S-020	п.10.2 [a11]	Сообщения-уведомления о завершении соединения	О
WTLS-S-021	п.10.2 [a11]	Сообщения-уведомления об ошибках, приводящих к завершению соединения	О
WTLS-S-022	п.10.2 [a11]	Контроль проверочной последовательности	О
WTLS-S-025	п.10.1 [a11]	Изменение способа шифрования	О
WTLS-S-026	п.9.2 [a11]	Данные, получаемые от вышестоящего уровня	О
WTLS-S-030	доп. А [a11]	Анонимная процедура handshake	О (поддержка одной из опций WTLS-S-031-038, 049)
WTLS-S-031	доп.А [a11]	Алгоритм DH без ограничения длины ключа	Опц.
WTLS-S-032	доп.А [a11]	Алгоритм DH с длиной ключа до 768 бит	Опц.
WTLS-S-033	доп.А [a11]	Алгоритм DH с длиной ключа до 512 бит	Опц.
WTLS-S-034	доп.А [a11]	Алгоритм RSA без ограничения длины ключа	Опц.
WTLS-S-035	доп.А [a11]	Алгоритм RSA с длиной ключа до 768 бит	Опц.
WTLS-S-036	доп.А [a11]	Алгоритм RSA с длиной ключа до 512 бит	Опц.
WTLS-S-037	доп.А [a11]	Алгоритм ECDH_ANON без ограничения длины ключа	Опц.
WTLS-S-038	доп.А [a11]	Алгоритм ECDH_ANON с длиной ключа до 131 бит	Опц.
WTLS-S-049	доп.А [a11]	Алгоритм ECDH_ANON с длиной ключа до 113 бит	Опц.
WTLS-S-060	доп. А [a11]	Неанонимная процедура handshake (сервер прошёл аутентификацию)	О (поддержка одной из опций WTLS-S-061, 064, 191)
WTLS-S-061	доп.А [a11]	Алгоритм RSA без ограничения длины ключа	Опц.
WTLS-S-062	доп.А [a11]	Алгоритм RSA с длиной ключа до 768 бит	Опц.
WTLS-S-063	доп.А [a11]	Алгоритм RSA с длиной ключа до 512 бит	Опц.
WTLS-S-064	доп.А [a11]	Алгоритм ECDH_ECDSA	Опц.
WTLS-S-070	доп. А [a11]	Аутентификация пользователя	О (поддержка одной из опций WTLS-S-071,072)
WTLS-S-071	доп.А [a11]	Алгоритм RSA без ограничения длины ключа	Опц.
WTLS-S-072	доп.А [a11]	Алгоритм ECDH_ECDSA	Опц.
WTLS-S-080	доп. А [a11]	Процедура shared secret handshake	Опц.
WTLS-S-090	доп.А [a11]	Использование нулевого ключа	Опц.
WTLS-S-100	доп. А [a11]	Шифрование данных пользователя	О (поддержка одной из опций WTLS-S-101-108)
WTLS-S-101	доп.А [a11]	Алгоритм RC5_CBC с эффективной длиной ключа 128 бит	Опц.
WTLS-S-102	доп.А [a11]	Алгоритм RC5_CBC_56 с эффективной длиной ключа 56 бит	Опц.
WTLS-S-103	доп.А [a11]	Алгоритм DES_CBC	Опц.

Продолжение таблицы 6.6

1	2	3	4
WTLS-S-104	доп.А [a11]	Алгоритм 3DES_CBC_EDE	Опц.
WTLS-S-105	доп.А [a11]	Алгоритм IDEA_CBC с эффективной длиной ключа 128 бит	Опц.
WTLS-S-106	доп.А [a11]	Алгоритм IDEA_CBC_56 с эффективной длиной ключа 56 бит	Опц.
WTLS-S-107	доп.А [a11]	Алгоритм RC5_CBC_64 с эффективной длиной ключа 64 бита	Опц.
WTLS-S-108	доп.А [a11]	Алгоритм IDEA_CBC_64 с эффективной длиной ключа 64 бита	Опц.
WTLS-S-120	доп.А [a11]	Использование нулевого шифрования	Опц.
WTLS-S-130	доп. А [a11]	Опции кода аутентификации сообщения MAC	О (поддержка WTLS-S-131)
WTLS-S-131	доп.А [a11]	Алгоритм SHA	Опц.
WTLS-S-132	доп.А [a11]	Алгоритм SHA_80	Опц.
WTLS-S-133	доп.А [a11]	Алгоритм SHA_40	Опц.
WTLS-S-134	доп.А [a11]	Алгоритм SHA_XOR_40	Опц.
WTLS-S-135	доп.А [a11]	Алгоритм MD5	Опц.
WTLS-S-136	доп.А [a11]	Алгоритм MD5_80	Опц.
WTLS-S-137	доп.А [a11]	Алгоритм MD5_40	Опц.
WTLS-S-140	доп.А [a11]	Использование нулевого ключа MAC	Опц.
WTLS-S-141	доп.А [a11]	Использование нулевого сжатия	Опц.
WTLS-S-151	доп.А [a11]	Использование предварительно определённых параметров группы 1 для алгоритма DH	Опц.
WTLS-S-152	доп.А [a11]	Использование предварительно определённых параметров группы 2 для алгоритма DH	Опц.
WTLS-S-165	доп. А [a11]	Характеристика 5 (163 бит)	Опц.
WTLS-S-167	доп. А [a11]	Характеристика 7 (160 бит)	Опц.
WTLS-S-161	доп. А [a11]	Небазисные характеристики алгоритмов семейства ECC (ECDH_xxxx). Характеристика 1 (113 бит)	Опц.
WTLS-S-163	доп. А [a11]	Характеристика 3 (163 бит)	Опц.
WTLS-S-164	доп. А [a11]	Характеристика 4 (113 бит)	Опц.
WTLS-S-166	доп. А [a11]	Характеристика 6 (112 бит)	Опц.
WTLS-S-168	доп. А [a11]	Характеристика 8 (112 бит)	Опц.
WTLS-S-169	доп. А [a11]	Характеристика 9 (160 бит)	Опц.
WTLS-S-170	доп. А [a11]	Характеристика 10 (233 бит)	Опц.
WTLS-S-171	доп. А [a11]	Характеристика 11 (233 бит)	Опц.
WTLS-S-172	доп. А [a11]	Характеристика 12 (224 бит)	Опц.
WTLS-S-180	п.11.1.3 [a11]	Точечное сжатие с использованием алгоритмов семейства ECC	Опц
WTLS-S-191	п.10.5.2 [a11]	Проверка наличия сертификатов алгоритмов. Сертификат WTLS (должен поддерживаться при анонимной процедуре handshake)	Опц. (поддержка WTLS-S-210)
WTLS-S-192	п.10.5.2 [a11]	Сертификат X.509	Опц.
WTLS-S-193	п.10.5.2 [a11]	Сертификат X.9.68	Опц.
WTLS-S-200	п.10.5.1 [a11]	Стандартное представление времени в UNIX	О
WTLS-S-210	п.10.5.1 [a11]	Отклонение недопустимого значения сертификата WTLS в случае, когда T=ca не присутствует	Опц.

6.2.7 Требования к поддержке функций протокола датаграмм (WDP) для WAP версии 2.0 должны соответствовать технической спецификации WAP-259 – WDP-20010614-a. Wireless Datagram Protocol [a16]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.7. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.17.

Таблица 6.7

Условное обозначение	Соответствие [a16]	Наименование функции	Обязательность поддержки
1	2	3	4
WDP-S-001	Прил.А к [a16]	Функции взаимодействия с сетями сухопутной подвижной радиосвязи	О (поддержка одной из опций WDP-CT-S-003-005, 009-010)
WDP-S-002	см.п.5.1.18	Поддержка протокола WCMP	Опц.
WDP-PF-S-001	п.6.3.1.1 [a16]	Использование примитива T-DUnidata.Reg	О
WDP-PF-S-002	п.6.3.1.1 [a16]	Использование примитива T-DUnidata.Ind	О
WDP-PF-S-003	п.6.3.1.2 [a16]	Использование примитива T-DError.Ind	Опц.
WDP-CT-S-003		Взаимодействие с пейджинговыми системами, использующими протокол FLEX™	Опц.
WDP-CT-S-004		Взаимодействие с сетями сотовой подвижной связи стандарта GSM900/1800	Опц.
WDP-CT-S-005		Взаимодействие с сетями сотовой подвижной связи стандарта DAMPS (TIA/EIA-136)	Опц.
WDP-CT-S-009		Взаимодействие с сетями транкинговой подвижной связи стандарта TETRA	Опц.
WDP-CT-S-010		Взаимодействие с сетями радиотехнологии DECT	Опц.
WDP-NA-S-001		Поддержка схемы адресования согласно рек.ITU-T E.164	Опц.
WDP-NA-S-002		Поддержка схемы адресования согласно рек.ITU-T X.25	Опц.
WDP-NA-S-003		Поддержка схемы адресования согласно спецификаций IPv4	Опц.
WDP-NA-S-004		Поддержка схемы адресования согласно спецификаций IPv6	Опц.
WDP-NA-S-006	п.6.1 [a16]	Поддержка схемы адресования порта назначения	О
WDP-NA-S-007	п.6.1 [a16]	Поддержка схемы адресования порта – источника	О
WDP-NA-S-008		Поддержка схемы адресования TETRA	Опц.
<b>Взаимодействие с сетями сотовой подвижной связи стандарта GSM900/1800</b>			
WDP-GSM-S-000		Поддержка услуги доставки информации GSM	Опц (поддержка WDP-CT-S-004 и одной из опций WDP-GSM-S-001, 005-009)
WDP-GSM-S-001		Услуга доставки информации с помощью GSM SMS	Опц.

Продолжение таблицы 6.7

1	2	3	4
WDP-GSM-S-002	п. 6.3.3 [a16]	Поддержка заголовка текста GSM SMS фазы 1	Опц.
WDP-GSM-S-003		Передача информационного элемента long fragmentation	Опц.
WDP-GSM-S-004		Передача информационного элемента short fragmentation	Опц.
WDP-GSM-S-005		Дополнительная услуга передачи неструктурированных данных USSD	Опц.
WDP-GSM-S-006		Информационные элементы услуги доставки данных USSD	Опц.
WDP-GSM-S-007		Услуга передачи данных в режиме с коммутацией пакетов GPRS	Опц.
WDP-GSM-S-008		Услуга передачи данных в режиме с коммутацией каналов	Опц.
WDP-GSM-S-009		Услуга передачи данных в режиме Cell broadcast	Опц.
WDP-GSM-S-010		Приём информационного элемента long fragmentation	Опц.
WDP-GSM-S-011		Приём информационного элемента short fragmentation	Опц.
<b>Взаимодействие с сетями сотовой подвижной связи стандарта DAMPS (TIA/EIA-136)</b>			
WDP-ANSI-S-000		Поддержка услуги доставки информации DAMPS	Опц. (поддержка WDP-CT-S-005 и одной из опций WDP-ANSI-S-001-004)
WDP-ANSI-S-001	TIA/EIA 136-750	Поддержка услуги R-DATA	Опц.
WDP-ANSI-S-002	TIA/EIA 136-370	Поддержка передачи данных в режиме с коммутацией пакетов	Опц.
WDP-ANSI-S-003	TIA/EIA 136-350	Поддержка передачи данных в режиме с коммутацией каналов	Опц.
WDP-ANSI-S-004	TIA/EIA 136-711	Поддержка услуги R-DATA с использованием GHOST	Опц.
WDP-ANSIBEAR-S-001	TIA/EIA 136-711	Передача информационного элемента long fragmentation	Опц.
WDP-ANSIBEAR-S-002	TIA/EIA 136-711	Передача информационного элемента short fragmentation	Опц.
WDP-ANSIBEAR-S-003	TIA/EIA 136-711	Приём информационного элемента long fragmentation	Опц.
WDP-ANSIBEAR-S-004	TIA/EIA 136-711	Приём информационного элемента short fragmentation	Опц.
<b>Взаимодействие с сетями транкинговой подвижной связи стандарта TETRA</b>			
WDP-TETRA-S-001	пп.4.4.10.1, 6.9 [a16]	Поддержка услуги SDS	Опц.
WDP-TETRA-S-002	пп.4.4.10.2, 6.2 [a16]	Поддержка услуги передачи данных с коммутацией пакетов	Опц.
<b>Взаимодействие с сетями радиотехнологии DECT</b>			
WDP-DECT-S-001	пп.4.4.11.1, 6.3.1, 6.3.2 [a16]	Поддержка услуги DECT SMS	Опц.

Продолжение таблицы 6.7

1	2	3	4
WDP-DECT-S-002	пп.4.4.11.2, 6.2 [a16]	Поддержка услуги передачи данных в режиме с установлением соединения	Опц.
WDP-DECT-S-003	пп.4.4.11.3, 6.2 [a16]	Поддержка услуги передачи данных в режиме с коммутацией пакетов	Опц.
<b>Взаимодействие с лейджинговыми системами, использующими протокол FLEX™</b>			
WDP-FLEX-S-001	пп.4.4.7, 6.6 [a16]	Поддержка протокола FLEX™	Опц.
WDP-FLEX-S-002	пп.4.4.7, 6.6 [a16]	Поддержка протокола ReFLEX™	Опц.

6.2.8 Требования к поддержке функций протокола транспортного уровня TLS должны соответствовать технической спецификации WAP-219 – TLS-20010411-a. TLS Profile and Tunneling [a17]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.8.

Таблица 6.8

Условное обозначение	Соответствие [a17]	Наименование функции	Обязательность поддержки
1	2	3	4
TLS-001	[a3]	Поддержка TLS 1.0	О
TLS-S-011	п.6.1 [a17]	Поддержка средства шифрования TLS_RSA_WITH_RC4_128_SHA	О
TLS-S-013	п.6.1 [a17]	Поддержка средства шифрования TLS_RSA_WITH_3DES_EDE_CBC_SHA	О
TLS-S-020	п.6.2 [a17]	Режим завершения сеанса	О
TLS-S-030	п.6.3 [a17]	Аутентификация сервера	О (поддержка одной из опций TLS-S-031, 032)
TLS-S-031	п.6.3 [a17], [a18]	Использование сертификата X.509 адаптированного для WAP	Опц.
TLS-S-032	п.6.3 [a17], [a19]	Использование сертификата X.509	Опц.
TLS-S-040	п.6.4 [a17]	Аутентификация пользователя	Опц. (поддержка опций TLS-S-100-103)
TLS-S-100	п.6.4 [a17], [a18]	Использование сертификата X.509 адаптированного для WAP	Опц.
TLS-S-101	п.6.4 [a17], [a19]	Использование сертификата X.509	Опц.
TLS-S-102	п.6.4 [a17]	Использование сертификата и электронной подписи RSA	Опц.
TLS-S-103	п.6.4 [a17]	Запрос типа сертификата RSA с целью идентификации пользователя	Опц.

6.2.9 Требования к поддержке функций протокола управления состоянием HTTP (HTTPSM) должны соответствовать технической спецификации WAP-223 – HTTPSM-20001213-a. HTTP State Management Specification [a20]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.9.



Таблица 6.9

Условное обозначение	Соответствие [a20]	Наименование функции	Обязательность поддержки
1	2	3	4
HSM-S001	п.9.1 [a20]	Поддержка промежуточной программой-агентом (Cookie Proxy) передачи заголовков HTTP между программой-агентом пользователя и сервером-инициатором обмена без каких-либо изменений	О
HSM-S002	п.9.2 [a20]	Управление промежуточной программой-агентом данными о состоянии и их хранение	Опц.
HSM-S003	п.9.2 [a20]	Выполнение функций программы-агента пользователя при взаимодействии с сервером-инициатором обмена	Опц. (при поддержке опции HSM-S002)
HSM-S004	п.9.2 [a20]	Поддержка промежуточной программой-агентом заголовков и процедур, используемых для управления состояниями HTTP при использовании WAP	Опц. (при поддержке опции HSM-S002)
HSM-S005	п.9.2 [a20]	Невозможность хранения промежуточной программой-агентом данных о состоянии HTTP в случае, когда сервером-инициатором обмена в заголовок Set-Cookie включён атрибут secure	Опц. (при поддержке опции HSM-S002)
HSM-S006	п.9.3 [a20]	Установление промежуточной программой-агентом связи данных о состоянии HTTP с конкретным пользователем и невозможность обработки или хранения данных об анонимных пользователях	Опц. (при поддержке опции HSM-S002)
HSM-S007	п.9.4 [a20]	Поддержка промежуточной программой-агентом пользовательского интерфейса для обработки данных состоянии HTTP	Опц.

6.2.10 Требования к формату сообщений, передаваемых по инициативе сервера содержания (технология push) должны соответствовать технической спецификации WAP-251 – PushMessage -20010322-a. Push Message [a21]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.10.

Таблица 6.10

Условное обозначение	Соответствие [a21]	Наименование функции	Обязательность поддержки
1	2	3	4
MSG-GEN-S-001	п.5.2.1 [a21]	Общий формат заголовка	Опц.
MSG-GEN-S-002	п.5.2.1.10 [a21]	Поддержка заголовка Content-Type	О
MSG-GEN-S-003	п.5.2.2 [a21]	Поддержка заголовков WAP	Опц.
MSG-GEN-S-004	п.5.2.3 [a21]	Поддержка расширения заголовков	Опц.
MSG-GEN-S-005	п.5.3 [a21]	Тело сообщения	Опц.
MSG-GEN-S-006	п.5.3 [a21]	Поддержка невложенных многочастевых содержаний	Опц.

Продолжение таблицы 6.10

1	2	3	4
MSG-GEN-S-007	п.5.3 [a21]	Поддержка вложенных многочастевых содержаний	Опц.
MSG-GEN-S-008	п.6 [a21]	Правило обработки заголовков	О

6.2.11 Требования к протоколу Push OTA должны соответствовать технической спецификации WAP-235 – PushOTA -20010425-a. Push OTA Protocol [a22]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.11.

Таблица 6.11

Условное обозначение	Соответствие [a22]	Наименование функции	Обязательность поддержки
1	2	3	4
OTA-CL-S-001	пп.5, 6.2.1 [a22]	Передача информации push в режиме без установления соединения	О
OTA-CO-S-001	п.5 [a22]	Передача информации push в режиме с установлением соединения	Опц.
OTA-CO-S-002	п.6.2.2 [a22]	Передача информации push в режиме с установлением соединения и использованием OTA-WSP	Опц. (при поддержке опции OTA-WSP-S-001 или 002-003 или 004-005)
OTA-WSP-S-001	п.6.2.2 [a22]	Передача информации push в режиме с подтверждением	Опц. (при поддержке опции WSP-CO-S-001 и 011)
OTA-WSP-S-002	п.6.2.2 [a22]	Передача информации push в режиме без подтверждения	Опц. (при поддержке опции WSP-CO-S-001 и 010)
OTA-WSP-S-003	п.6.2.2 [a22]	Использование незащищенной передачи информации push	Опц.
OTA-WSP-S-004	п.6.2.2 [a22]	Использование защищенной передачи информации push	Опц. (при поддержке WTLS – см.п.6.2.6)
OTA-WSP-S-005	пп.8, 8.2, 8.4 [a22]	Использование запроса инициализации сеанса для передачи контента инициализации сеанса SIA/SIR	Опц.
OTA-WSP-S-006	п.6.2.3 [a22]	Передача информации push по идентификатору прикладной программы	О
OTA-WSP-S-007	п.6.2.4 [a22]	Аутентификация сервера инициировавшего соединение	Опц.
OTA-WSP-S-008	п.6.2.6 [a22]	Выбор системы передачи информации push сервером	Опц.
OTA-WSP-S-009	п.6.2.6 [a22]	Контроль системы передачи информации push сервером	Опц.
OTA-CO-S-003	п.7 [a22]	Передача информации push в режиме с установлением соединения и использованием OTA-HTTP	Опц. (при поддержке опции OTA-HTTP-S-001, 007-012, 014-015), HTTP-S-C001

Продолжение таблицы 6.11

1	2	3	4
OTA-HTTP-S-001	п.7.2.4.1 [a22]	Режим установления соединения с использованием TCP по инициативе терминала TO-TCP	Опц.
OTA-HTTP-S-002	п.7.2.4.1 [a22]	Режим установления соединения с использованием TCP по инициативе шлюза PPG PO-TCP	Опц.
OTA-HTTP-S-003	п.7.2.4.1 [a22]	Режим установления соединения с использованием TCP и защищённой передачей (OTA_HTTP-TLS) по инициативе терминала TO-TCP	Опц. (при поддержке об.функций TLS – см.п.6.2.8)
OTA-HTTP-S-004	п.7.2.4.1 [a22]	Режим установления соединения с использованием TCP и защищённой передачей (OTA_HTTP-TLS) по инициативе терминала TO-TCP	Опц. (при поддержке об.функций TLS – см.п.6.2.8)
OTA-HTTP-S-005	пп.7.2.5, 7.2.5.1 [a22]	Режим регистрации терминала шлюзом PPG с использованием метода OPTIONS	Опц.
OTA-HTTP-S-006	пп.7.2.5, 7.2.5.2 [a22]	Режим проверки регистрации терминала шлюзом PPG с использованием метода POST	Опц.
OTA-HTTP-S-007	п.7.2.6.1 [a22]	Использование шлюзом PPG идентификационных данных, полученных в ответ на запрос регистрации (OTA-HTTP-S-005)	Опц.
OTA-HTTP-S-008	п.7.2.6.2 [a22]	Использование шлюзом PPG идентификационных данных, полученных в ответ на запрос регистрации (OTA-HTTP-S-006)	Опц.
OTA-HTTP-S-009	п.7.2.6.2 [a22]	Возможность идентификации шлюза PPG терминалом	Опц.
OTA-HTTP-S-010	п.7.3 [a22]	Способ адресования приложений	Опц.
OTA-HTTP-S-011	п.7.4 [a22]	Доставка информации push с использованием метода HTTP POST	Опц.
OTA-HTTP-S-012	п.7.5 [a22]	Обработка данных о номере версии протокола	Опц.
OTA-HTTP-S-013	п.8.3 [a22]	Использование таймера блокировки в целях защиты от несанкционированного доступа	Опц.
OTA-HTTP-S-014	п.7.6 [a22]	Обработка данных о доступном способе доставки информации	Опц.
OTA-HTTP-S-015	п.7.2.5.4 [a22]	Поддержка заголовка X-Wap-Push-ProxyURL	Опц.

6.2.12 Требования к индикации услуги с использованием радиотехнологии push (Service Indication) декларируются фирмой-изготовителем в объёме, определённом п.5.1.7 (табл.5.7).

6.2.13 Требования к реализации функций шлюза push (Push Proxy Gateway – PPG) должны соответствовать технической спецификации WAP-249 – PPGService -20010713-а. Push Proxy Gateway Service [a23]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.12.

Таблица 6.12

Условное обозначение	Соответствие [a23]	Наименование функции	Обязательность поддержки
1	2	3	4
PPG-CO-S-001		Поддержка передачи информации push в режиме с подтверждением	Опц. (при поддержке опции OTA-CO-S-002 или 003, и PPG-GEN-S-013)
PPG-GEN-S-001	п.5.1.1 [a23]	Отказ в передаче информации push с недопустимым содержанием элемента PAP push-message	О
PPG-GEN-S-002	п.5.1.1 [a23]	Уведомление о незавершенности передачи информации push	О
PPG-GEN-S-003	п.5.1.2.1.1 [a23]	Недопустимость трансформации содержания информации, в отношении которой действует ограничение в соответствии с [a7]	О
PPG-GEN-S-004	п.5.1.2.1.1 [a23]	Проверка заголовка трансформированной информации	О
PPG-GEN-S-005	п.5.1.2.1.2 [a23]	Обработка заголовка X-Wap-Application-Id	О
PPG-GEN-S-006	п.5.1.2.1.2 [a23]	Передача заголовка X-Wap-Application-Id через радиointерфейс в цифровом формате	О
PPG-GEN-S-007	п.5.1.2.1.3 [a23]	Использование атрибута message-state	О
PPG-GEN-S-008	п.5.1.2.2.2 [a23]	Выбор системы связи и/или в сети в соответствии с разделом QOS элемента PAP push-message	О
PPG-GEN-S-009	п.5.1.2.2.3 [a23]	Уведомление о неуспешной активизации или выборе соединения сеансового уровня	О
PPG-GEN-S-010	п.5.1.2.2.4 [a23]	Использование ограничений по времени доставки информации	О
PPG-GEN-S-011	п.5.1.2.2.5 [a23]	Использование атрибута delivery-method	О
PPG-GEN-S-012	п.5.1.2.2.5.1 [a23]	Уведомление о передаче сообщения push в режиме без подтверждения с использованием OTA-HTTP	О
PPG-GEN-S-013	п.5.1.2.2.5.2 [a23]	Уведомление о передаче сообщения push в режиме с подтверждением	Опц.
PPG-GEN-S-014	п.5.2 [a23]	Передача сообщения resultnotofocation-message	О
PPG-GEN-S-015	п.5.3 [a23]	Реакция на сообщения statusquery-message	Опц.
PPG-GEN-S-016	п.5.4 [a23]	Отмена доставки информации push с получением сообщения PAP cancel-message	Опц.
PPG-GEN-S-017	п.5.4 [a23]	Обработка сообщений PAP cancel-message	О
PPG-GEN-S-018	п.5.1.2.1.1.1 [a23]	Преобразование заголовка в соответствии с требованиями п.6.2.10	О
PPG-GEN-S-019	п.5.1.2.1.1.2 [a23]	Кодирование заголовка в соответствии с RFC1951 [a24]	Опц. (при поддержке опции OTA-CO-S-003)

Продолжение таблицы 6.12

1	2	3	4
PPG-GEN-S-020	п.5.1.1.1 [a23]	Замена сообщения push в соответствии с запросом PAP push-message	Опц.
PPG-GEN-S-021	п.5.1.2.1.1.1 [a23]	Кодирование заголовка в соответствии с WSP-CO-S-014, 015 (п.6.2.4) при использовании WSP	О
PPG-GEN-S-022	п.5.1.2.1.1.1 [a23]	Кодирование контента в соответствии с требованиями п.5.1.4	О
PPG-GEN-S-023	п.5.1.2.1.1.2 [a23]	Кодирование контента в соответствии с требованиями RFC1951 [a24]	Опц.
PPG-ADD-S-001	п.7 [a23]	Идентификация получателей информации push	О
PPG-ADD-S-002	п.7 [a23]	Поддержка идентификаторов, определённых пользователями информации push	Опц.
PPG-ADD-S-003	п.7 [a23]	Поддержка идентификаторов устройств	Опц.
PPG-ADD-S-004	п.7 [a23]	Обработка сервером адресов пользователей	О

6.2.14 Требования к протоколу доступа для технологии push (Push Access Protocol – PAP) должны соответствовать технической спецификации WAP-247 – PAP -20010429-а. Push Access Protocol [a25]. В рамках сертификации фирм-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.13.

Таблица 6.13

Условное обозначение	Соответствие [a25]	Наименование функции	Обязательность поддержки
1	2	3	4
PAP-VAL-S-001	п.5.1 [a25]	Проверка управляющего объекта сообщения push message и уведомление инициатора передачи о результатах проверки	О
PAP-VAL-S-001	п.5.1 [a25]	Проверка содержания сообщения push message	Опц.
PAP-VAL-S-001	п.5.1 [a25]	Проверка адресов	Опц.
PAP-OPS-S-001	п.5.1 [a25]	Передача информации (push submission)	О
PAP-OPS-S-002	п.5.2 [a25]	Уведомление инициатора передачи о результатах передачи информации мобильному абоненту	О
PAP-OPS-S-003	п.5.3 [a25]	Отмена передачи информации мобильному абоненту со стороны сервера-инициатора	Опц.
PAP-OPS-S-004	п.5.4 [a25]	Обработка запросов о статусе информации адресованной мобильному абоненту со стороны сервера-инициатора	Опц.
PAP-OPS-S-005	п.5.5 [a25]	Обработка запросов о возможностях мобильного абонента по приёму адресованной ему информации со стороны сервера-инициатора	Опц.
PAP-SEM-S-001	п.6.1 [a25]	Поддержка режима обработки информации, предназначенной для передачи в адрес нескольких мобильных абонентов	Опц.
PAP-SEM-S-002	п.6.1 [a25]	Уведомление о результатах доставки информации, переданной в адрес нескольких мобильных абонентов	Опц.

Продолжение таблицы 6.13

1	2	3	4
PAP-SEM-S-003	п.8.2 [a25]	Доставка информации после заданного времени	Опц.
PAP-SEM-S-004	п.8.2 [a25]	Доставка информации до заданного времени	Опц.
PAP-SEM-S-005	п.8.2.2 [a25]	Отклонение запроса доставки информации в случае, когда её невозможно осуществить с заданным качеством (QOS)	О
PAP-SEM-S-006	п.8.2.2 [a25]	Использование атрибута delivery-method=	О
PAP-SEM-S-007	п.8.2.2 [a25]	Использование атрибута priority=	Опц.
PAP-SEM-S-008	п.8.3 [a25]	Использование элемента progress-note	Опц.
PAP-SEM-S-009	п.5.1 [a25]	Обработка запросов о возможностях мобильного абонента по приёму адресованной ему информации со стороны сервера-инициатора, содержащихся в сообщении push-message	Опц.
PAP-SEM-S-010	п.8.12 [a25]	Использование статус кода 3002 для инициатора передачи информации только в случае, когда версия PAP не поддерживается	О
PAP-SEM-S-011	п.8.12 [a25]	Обнаружение версии PAPв принятом сообщении.	О
PAP-SEM-S-012	п.9.2 [a25]	Использование инструкции по обработке сообщения, полученного от инициатора push в случае использования версии протокола PAP, отличной от 1.0.	О
PAP-SEM-S-013	п.9.2 [a25]	Уведомление о поддерживаемых версиях протокола в случае, когда получена инструкция по обработке сообщения.	О
PAP-SEM-S-014	п.9.3 [a25]	Поддержка передачи сообщения bedmessage-response протокола версии 1.0 со статус кодом 3002 в случае когда данная версия протокола не поддерживается.	О
PAP-SEM-S-015	п.9.5 [a25]	Сохранение версии протокола аналогичной полученной от инициатора push	О
PAP-SEM-S-016	п.8.2 [a25]	Возможность замены сообщения по инициативе инициатора push	Опц.

#### 6.2.15 Поддержка услуги приёма/передачи мультимедийных сообщений (MMS)

Услуга приёма/передачи мультимедийных сообщений (Multimedia Messaging Service – MMS) предоставляет возможность получения/отправки абонентом сети подвижной радиосвязи расширенной номенклатуры сообщений, включающей в себя в соответствии с [a26]:

текстовые сообщения на основе различных символьных кодировок;

сообщения, представляющие собой аудиосигналы, образованные путём использования различных алгоритмов цифровой обработки аудиосигналов;

сообщения, представляющие собой неподвижные изображения в виде графических файлов различных форматов;

сообщения, представляющие собой подвижные изображения, образованные путём использования различных алгоритмов цифровой обработки видеосигналов.

Поддержка услуги приёма/передачи мультимедийных сообщений предусматривает наличие:

прикладных средств обработки мультимедийных сообщений в абонентском устройстве (оконечном оборудовании пользователя) – программы-агента пользователя MMS;

средств хранения и обработки мультимедийных сообщений (серверов/ретрансляторов MMS), входящих в состав сети подвижной радиосвязи и обеспечивающих сопряжение между программой-агентом пользователя и внешними серверами, осуществляющими генерирование, хранение и распространение мультимедийных сообщений.

Передача мультимедийных сообщений в сетях подвижной радиосвязи осуществляется с использованием протокола WAP [a27, a28]. Вариант сети подвижной радиосвязи с поддержкой MMS представлен на рис.7.

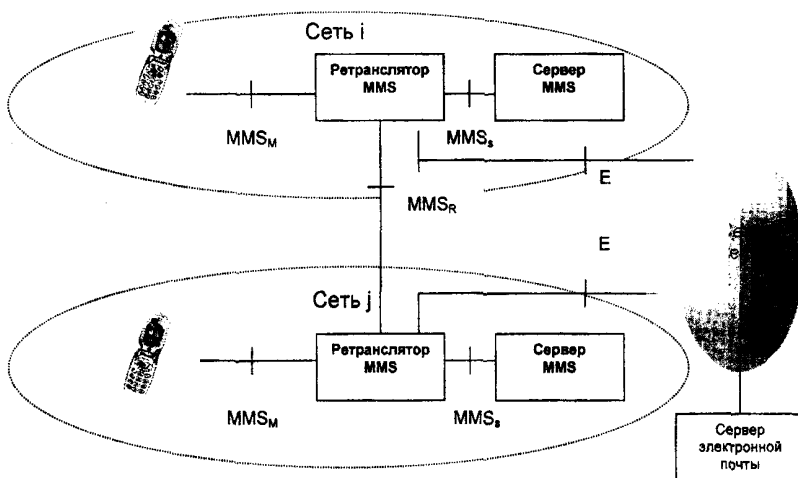


Рис.7.

Передача мультимедийных сообщений с использованием WAP осуществляется в следующей последовательности:

а) Абонент сети подвижной связи инициирует передачу мультимедийного сообщения через интерфейс  $MMS_M$  (в сетях сотовой подвижной связи используется также обозначение  $MM1$  [a27]) в адрес ретранслятора MMS. Интерфейс  $MMS_M$  использует в качестве протоколов нижних уровней стандартные протоколы сетей подвижной связи в зависимости от используемого стандарта. В качестве протоколов транспортного уровня используется WSP (метод POST) (см. п.п. 5.1.13, 6.2.4) и/или HTTP (метод POST) (см. п. 6.2.3).

б) Ретранслятор/сервер MMS осуществляет обработку сообщения, полученного от абонента сети и:

- посылает его в виде сообщения электронной почты пользователю фиксированной сети Internet через интерфейс E, соответствующий [a43] с использованием схемы адресования SMTP [a29] и формата MIME [a30] для передачи самого сообщения.

- посылает уведомление о наличии адресованного ему мультимедийного сообщения подвижному абоненту своей сети через интерфейс MMS<sub>M</sub> или другой сети подвижной связи через интерфейс MMS<sub>R</sub> (в сетях сотовой подвижной связи используется также обозначение MM3 [a27]), с указанием соответствующего идентификатора ресурса (URI). Одним из наиболее распространённых методов посылки уведомления является использование технологии push (см. пп.5.1.7, 6.2.10-6.2.14) посредством услуги коротких сообщений (SMS).

Примечание: Интерфейс MMS<sub>R</sub> (в сетях сотовой подвижной связи MM2) является, как правило, внутренним и обеспечивает взаимодействие ретранслятора, осуществляющего обработку сообщений и сервера, основным назначением которого является хранение сообщений.

в) После получения уведомления программа-агент пользователя в абонентском устройстве инициирует запрос с целью получения сообщения с сервера, используя WSP (метод GET) (см.пп.5.1.13, 6.2.4) и/или HTTP (метод GET) (см.п.6.2.3).

г) После получения подтверждения получения сообщения, ретранслятор/сервер MMS осуществляет уведомление отправителя о доставке мультимедийного сообщения.

Настоящие технические требования распространяются на шлюзы WAP, обеспечивающие поддержку MMS, серверы/ретрансляторы MMS, а также серверы, объединяющие в себе перечисленные функции.

6.2.15.1 Техническая реализация интерфейса MMS<sub>M</sub> с использованием шлюзов WAP версии 1.2.

Архитектура протокола интерфейса MMS<sub>M</sub> при поддержке услуги передачи мультимедийных сообщений в сети, использующей шлюз WAP версии семейства 1.x (1.2 и последующих), представлена на рис.8.

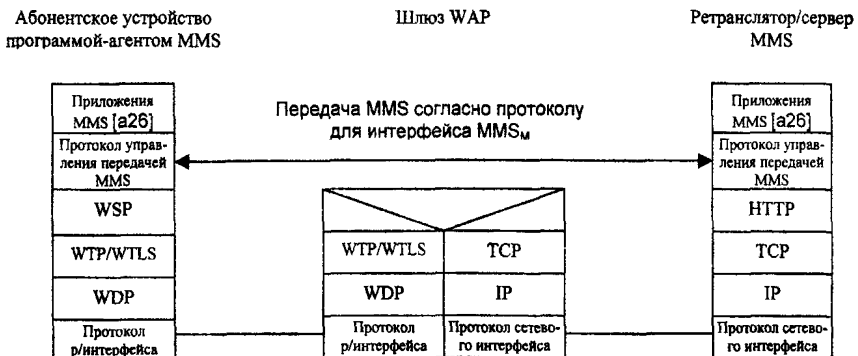


Рис.8



В случае использования шлюза WAP версии 1.x, обеспечивается трансформация протокола HTTP для фиксированной сети в WAP WSP, а управление передачей MMS осуществляется ретранслятором/сервером MMS и программой-агентом в абонентском устройстве.

Требования к шлюзу WAP для данной конфигурации сети устанавливаются в объеме раздела 5.

6.2.15.2 Техническая реализация интерфейса MMS<sub>M</sub> с использованием шлюзов WAP версии 2.0.

Архитектура протокола интерфейса MMS<sub>M</sub> при поддержке услуги передачи мультимедийных сообщений в сети, использующей шлюз WAP версий семейства 2.0, приведена на рис.9.

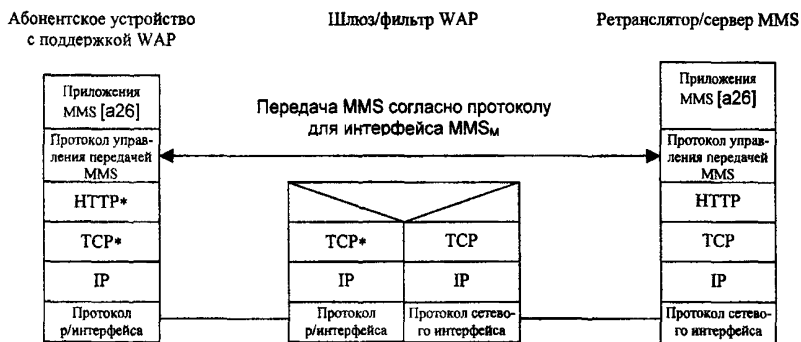


Рис.9

В случае использования шлюза WAP версии 2.0, обеспечивается трансформация протокола HTTP для фиксированной сети в протокол HTTP\* для подвижной сети, а управление передачей MMS осуществляется ретранслятором/сервером MMS и программой-агентом в абонентском устройстве.

Требования к шлюзу WAP для данной конфигурации сети устанавливаются в объеме раздела 6.

6.2.15.3 Требования к ретранслятору/серверу MMS в части реализации требований к протоколу управления передачей MMS.

6.2.15.3.1 Требования к транзакциям ретранслятора MMS и пользователей услуги должны соответствовать технической спецификации WAP-206 MMSCTR –20020115-a. MMS Client Transactions. [a31]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.14.

Таблица 6.14

Условное обозначение	Соответствие [a31]	Наименование функции	Обязательность поддержки
1	2	3	4
MMSC-TR-SLF-S-001	п.п. 8, 9 [a31]	Согласование возможностей между программой-агентом пользователя и ретранслятором MMS	Опц. (при поддержке обязательных опций [a32])
MMSC-TR-SND-S-001	п. 7.1 [a31]	Транзакция Send между пользователем MMS-отправителем сообщения и ретранслятором MMS	О
MMSC-TR-SND-S-002	п. 7.1.1 [a31]	Обработка запроса передачи мультимедийного сообщения M-send.req от пользователя.	Опц. (треб. поддержка MMSE-S-078, см. п. 6.2.15.3.2)
MMSC-TR-SND-S-003	п. 7.1.1 [a31]	Подтверждение запроса передачи мультимедийного сообщения M-send.conf от ретранслятора	Опц. (треб. поддержка MMSE-S-078, см. п. 6.2.15.3.2)
MMSC-TR-NTF-S-001	п. 7.2 [a31]	Транзакция Notification между ретранслятором MMS и пользователем MMS-получателем сообщения	О
MMSC-TR-NTF-S-002	п. 7.2.1 [a31]	Передача сообщения M-Notification.Ind для пользователя MMS от ретранслятора MMS	Опц. (треб. Поддержка MMSE-S-079, см. п. 6.2.15.3.2 и MMSC-TR-PSH-002)
MMSC-TR-NTF-S-003	п. 7.2.1 [a31]	Приём ответа M-NotifyResp.ind от пользователя MMS	Опц. (треб. Поддержка MMSE-S-079, см. п. 6.2.15.3.2)
MMSC-TR-FTC-S-001	п. 7.3 [a31]	Транзакция Retrieval между пользователем MMS-получателем сообщения и ретранслятором MMS	О
MMSC-TR-FTC-S-002	п. 7.3.1 [a31]	Обработка запроса передачи сообщения от пользователя MMS WSP/HTTP GET.req	Опц.
MMSC-TR-FTC-S-003	п. 7.3.1 [a31]	Передача подтверждения запроса и запрашиваемого сообщения M-retrieve.conf ретранслятором MMS	Опц. (треб. Поддержка MMSE-S-080, см. п. 6.2.15.3.2)
MMSC-TR-FTC-S-004	п. 7.3.1 [a31]	Запрос и получение подтверждения о получении сообщения от пользователя MMS-получателя сообщения Acknowledge.ind	Опц. (треб. Поддержка MMSE-S-080, см. п. 6.2.15.3.2)
MMSC-TR-DRP-S-001	п. 7.4 [a31]	Транзакция Delivery Report между ретранслятором MMS и пользователем MMS-отправителем сообщения	О
MMSC-TR-DRP-S-002	п. 7.4.1 [a31]	Передача отчёта о доставке сообщения пользователю MMS - отправителю сообщения MMS M-Delivery.ind	Опц. (треб. поддержка MMSE-S-081, см. п. 6.2.15.3.2 и MMSC-TR-PSH-002)

Продолжение таблицы 6.14

1	2	3	4
MMSC-PSH-S-002	пп.7.2.1, 7.4.1 [a31]	Используемые типы и содержание сообщений push	Опц. (треб. поддержка MSG-GEN-S-002, 003, 005 – см.п.6.2.10)

6.2.15.3.2 Требования к протоколу инкапсуляции MMS должны соответствовать спецификации WAP-209 MMSEncapsulation –20020105-а. MMS Encapsulation Protocol. [a33]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.15.

Таблица 6.15

Условное обозначение	Соответствие [a33]	Наименование функции	Обязательность поддержки
1	2	3	4
MMSE-S-078	п.6.1 [a33]	Приём сообщения M-send.req	О
MMSE-S-079	п.6.1 [a33]	Передача уведомления M-Notification.ind	О
MMSE-S-080	п.6.1 [a33]	Доставка сообщения M-Retrieve.conf	О
MMSE-S-081	п.6.5 [a33]	Формирование и доставка отчёта о доставке сообщения	О
MMSE-S-082	п.6.6 [a33]	Доставка сообщения Read-Reply	О
MMSE-S-083	п.6.3 [a33]	Указание даты в доставленном сообщении (поле Date сообщения M-Retrieve.conf)	О
MMSE-S-084	п.6.1.1 [a33]	Указание адреса отправителя (поля From сообщения M-send.req)	О
MMSE-S-085	пп.6.2, 6.3 [a31]	Поддержка возможности исключения поля From из сообщения M-Retrieve.conf в случае, когда отправитель запрашивает возможность сокрытия адреса отправителя	Опц.
MMSE-S-086	п.6.2 [a33]	Поддержка добавления поля Message-Class в сообщение M-Notification.ind, в случае, когда эти данные не передаются отправителем	О
MMSE-S-087	п.6.1.1 [a33]	Поддержка поля X-Mms-Expiry в сообщении M-Send.req	Опц.
MMSE-S-088	п.6.1.1 [a33]	Поддержка согласованной доставки в случае поддержки поля X-Mms-Delivery-Time в сообщении M-Send.req	Опц.
MMSE-S-089	п.6.1.1 [a33]	Поддержка ускоренной доставки в случае поддержки поля X-Mms-Priority в сообщении M-Send.req	Опц.
MMSE-CHS-S-001	п.7.2.9 [a33]	Поддержка символьной кодировки UTF-8	Опц.
MMSE-CHS-S-002	п.7.2.9 [a33]	Поддержка символьной кодировки UTF-16	Опц.
MMSE-CHS-S-003	п.7.2.9 [a33]	Поддержка символьной кодировки UCS-2	Опц.
MMSE-CHS-S-004	п.7.2.9 [a33]	Поддержка символьной кодировки UCS-4	Опц.
MMSE-CHS-S-005	п.7.2.9 [a33]	Поддержка прочих символьных кодировок	Опц.

6.2.16 Требования к способам кодирования контента, передаваемого в адрес абонента при использовании режима минимизации взаимодействия с пользователем (provisioning), должны соответствовать технической спецификации WAP-183 – ProvCont – 20010724-a. Provisioning Content [a34]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.16.

Таблица 6.16

Условное обозначение	Соответствие [a34]	Наименование функции	Обязательность поддержки
1	2	3	4
ProvCont-SG-S-001	п.8 [a34]	Кодирование с использованием формата WBXML (см.п.5.1.4)	О (треб. поддержка WBXML-1-2, 4-5, 6,8 см.п.5.1.4)

6.2.17 Требования к поддержке взаимодействия с серверами прикладных услуг беспроводной телефонии (серверами WTA) для WAP версии 2.0 должны соответствовать технической спецификации WAP-266 – WTA-20010908-a. WAP Wireless Telephony Application [a35]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, представленной в таблице 6.17. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.9.

Таблица 6.17

Условное обозначение	Соответствие [a35]	Наименование функции	Обязательность поддержки
1	2	3	4
WTA –NETT-S-001		Тип сети подвижной связи, с абонентами которой поддерживает взаимодействие шлюз WAP	О (треб. поддержка одной из опций WTA-GSM-S001, ANSI136-S-001 или ONETT-S-001)
WTA-GSM-S-001		Поддержка взаимодействия с абонентами сети GSM900/1800	Опц.
WTA-ANSI136-S-001		Поддержка взаимодействия с абонентами сети DAMPS (TIA/EIA-136)	Опц.
WTA-ONETT-S-001		Поддержка взаимодействия с абонентами других сетей	Опц. (треб. поддержка одной из опций WDP-TETRA-S-000, WDP-DECT-S-000 или WDP-FLEX-S-000 )
WTA-WAE-S-001	пп.4-6 [a35]	Поддержка общих функций, определяемых WAE	О (требуется поддержка обязательных функций согласно п.6.2.2)
WTA-FMT-S-001	п.7.2.4 [a35]	Поддержка символьных кодировок WBXML для форматов контента WTA-WML	Опц. (требуется поддержка обязательных функций согласно п.5.1.4)
WTA-FMT-S-002	п.8.4.1.7 [a35]	Поддержка символьных кодировок WBXML для форматов контента канала	О (требуется поддержка обязательных функций согласно п.5.1.4)

Продолжение таблицы 6.17

1	2	3	4
WTA-SEC-S-001	п.5.5 [a11]	Поддержка средств защиты от несанкционированного доступа класса 2	О (требуется поддержка обязательных функций согласно п.6.2.6)
WTA-SEC-S-002	п.5.2 [a36]	Защита от несанкционированного доступа к данным WTA на сеансовом уровне	О (требуется поддержка обязательных функций согласно п.6.2.6)
WTA-IF-S-001	[a36]	Поддержка функций сервера библиотек для услуг общего пользования и сетевых услуг	О (требуется поддержка обязательных функций согласно п.6.2.18)
WTA-IF-S-002	[a37]	Поддержка функций сервера библиотек для сети стандарта GSM	Опц. (требуется поддержка обязательных функций WTAIGSM-ENC-S-001-002 п.6.2.18)
WTA-IF-S-003	[a38]	Поддержка функций сервера библиотек для сети стандарта DAMPS (TIA/EIA-136)	Опц. (требуется поддержка обязательных функций WTAIANSI136-ENC-S-001-002 п.6.2.18)

6.2.18 Требования к поддержке интерфейса с прикладными услугами беспроводной телефонии для WAP версии 2.0 должны соответствовать техническим спецификациям WAP-268 – WTAI-20010908-a. WAP Wireless Telephony Application Interface [a36], WAP-255 – WTAIGSM-20010908-a. WAP Wireless Telephony Application Interface. GSM Specific Addendum [a37] WAP-269 – WTAIIS136-20010908. WAP Wireless Telephony Application Interface. ANSI136 Specific Addendum [a38]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанным спецификациям по форме, представленной в таблице 6.18. В случае реализации WAP версий 1.x. требования должны соответствовать п.5.1.10.

Таблица 6.18

Условное обозначение	Соответствие [a36-a38]	Наименование функции	Обязательность поддержки
1	2	3	4
WTAI-ENC-S-001	п.8 [a36]	Поддержка идентификатора библиотеки WTAI для услуг общего назначения	О (требуется поддержка обязательных функций согласно п.5.1.5)
WTAI-ENC-S-002	п.8 [a36]	Поддержка идентификаторов функций WTAI услуг общего назначения	
WTAI-ENC-S-003	п.9 [a36]	Поддержка идентификатора библиотеки для управления речевыми вызовами	
WTAI-ENC-S-004	п.9 [a36]	Поддержка идентификаторов функций управления речевыми вызовами	
WTAI-ENC-S-005	п.10 [a36]	Поддержка идентификатора библиотеки для управления сообщениями	
WTAI-ENC-S-006	п.10 [a36]	Поддержка идентификаторов функций управления сообщениями	
WTAI-ENC-S-007	п.11 [a36]	Поддержка идентификатора библиотеки для управления электронной записной книжкой	

Продолжение таблицы 6.18

1	2	3	4
WTAI-ENC-S-008	п.11 [a36]	Поддержка идентификаторов функций управления электронной записной книжкой	О (требуется поддержка обязательных функций согласно п.5.1.5)
WTAI-ENC-S-009	п.12 [a36]	Поддержка идентификатора библиотеки для управления записями, относящимися к вызовам	
WTAI-ENC-S-010	п.12 [a36]	Поддержка идентификаторов функций управления записями, относящимися к вызовам	
WTAI-ENC-S-011	п.13 [a36]	Поддержка идентификатора библиотеки для управления вспомогательными функц.	
WTAI-ENC-S-012	п.13 [a36]	Поддержка идентификаторов функций управления вспомогательными функциями	
WTAIGSM-ENC-S-001	п.7.2 [a37]	Поддержка идентификаторов библиотек WTAI для GSM	
WTAIGSM-ENC-S002	п.7.2 [a37]	Поддержка идентификаторов функций WTAI для GSM	
WTAIANSI136-ENC-S-001	п.5.2 [a38]	Поддержка идентификаторов библиотек WTAI для ANSI-136	
WTAIANSI136-ENC-S-002	п.5.2 [a38]	Поддержка идентификаторов функций WTAI для ANSI-136	

6.2.19 Требования к поддержке синхронизации данных должны соответствовать технической спецификации WAP-234 – SYNC –20010530-а. WAP Sync Spec. Data Synchronisation Specification [a39], а также приведенным в протоколах SyncML Sync Protocol, version 1.0 [a40], SyncML HTTP Binding, version 1.0 [a41], SyncML over WSP, Version 1.0 [a42]. В рамках сертификации фирма-изготовитель должна представить декларацию соответствия шлюза WAP указанной спецификации по форме, приведенной в таблице 6.19.

Таблица 6.19

Условное обозначение	Соответствие [a39-a42]	Наименование функции	Обязательность поддержки
1	2	3	4
SYNC-S-001	п.5.2 [a39], [a40]	Использование протокола SyncML для синхронизации данных	О (поддержка одной из опций SYNC-S-002 или 003)
SYNC-S-002	п.5.3 [a39], [a42]	Поддержка компоновки данных при помощи протокола SyncML WSP	Опц.
SYNC-S-003	п.5.3 [a39], [a41]	Поддержка компоновки данных при помощи протокола SyncML HTTP	Опц.

### 6.3 Требования к интерфейсам

Интерфейсы, обеспечивающие взаимодействие шлюза WAP, использующего протокол версии 2.0, и/или серверов/ретрансляторов MMS с аппаратурой доступа к сети IP (IWF), должны соответствовать разделу 3.5 [a43].

Конкретные типы используемых интерфейсов устанавливаются в Технических условиях.

#### 6.4 Требования электромагнитной совместимости

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям электромагнитной совместимости, установленным в п.5.3.

#### 6.5 Требования к электропитанию

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям к электропитанию, установленным в п.5.4.

#### 6.6 Требования по устойчивости к климатическим и механическим воздействиям

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям по устойчивости к климатическим и механическим воздействиям, установленным в п.5.5.

#### 6.7 Требования безопасности

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям безопасности, установленным в п.5.6.

#### 6.8 Требования к маркировке

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям к маркировке, установленным в п.5.7.

#### 6.9 Требования к упаковке

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям к упаковке, установленным в п.5.8.

#### 6.10 Требования к транспортированию и хранению

Шлюз WAP с версией протокола 2.0 и сервер/ретранслятор MMS должны соответствовать требованиям к транспортированию и хранению, установленным в п.5.9.

## ПРИЛОЖЕНИЕ А

### Библиография

- a1. WAP-225 – TCP-20010321-p. Wireless Profiled TCP Specification.
- a2. WAP-229 – HTTP-20010329-a. Wireless Profiled HTTP.
- a3. RFC2246 - The TLS Protocol Version 1.0, T. Dierks, C. Allen, January 1999
- a4. RFC2401 - Security Architecture for the Internet Protocol, S. Kent, R. Atkinson, November 1998.
- a5. WAP-262 – ClassConform-20020517-a. Class conformance Requirements.
- a6. WAP-236 – WAESpec-20020207-a. Wireless Application Environment Specification. Version 2.0.
- a7. RFC2616 – Hypertext Transfer Protocol – HTTP/1.1. R.Fielding, J.Gettys, ..., June 1999.
- a8. RFC2817 – Upgrading to TLS within HTTP/1.1. R Khare, S.Lawrence, May 2000.
- a9. RFC2396 - Uniform Resource Identifiers (URI): Generic Syntax, T. Berners-Lee, et al., August 1998.
- a10. WAP-219
- a11. WAP-261– WTLS-20010406-a. Wireless Transport Layer Security
- a12. RFC3023 XML Media Types, M. Murata et al., January 2001.
- a13. WAP-230 – WSP-20010705-a. Wireless Session Protocol Specification.
- a14. WAP-238
- a15. WAP-224 – WTP-20010710-a. Wireless Transaction Protocol.
- a16. WAP-259 – WDP-20010614-a. Wireless Datagram Protocol
- a17. WAP-219 – TLS-20010411-a. TLS Profile and Tunneling.
- a18. WAP-211 - WAPCert-20010522-a. WAP Certificate profile Specification.
- a19. RFC2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R. Housley, W.Ford, W. Polk, D. Solo, January 1999.
- a20. WAP-223 – HTTPSM-20001213-a. HTTP State Management Specification.
- a21. WAP-251 – PushMessage -20010322-a. Push Message.
- a22. WAP-235 – PushOTA -20010425-a. Push OTA Protocol.
- a23. WAP-249 – PPGService -20010713-a. Push Proxy Gateway Service.
- a24. DEFLATE Compressed Data Format Specification version 1.3. P. Deutsch. May 1996.
- a25. WAP-247 – PAP -20010429-a. Push Access Protocol.



- a26. ETSI TS 126 140 (v.5.0.0) (2002-03) Digital cellular telecommunication system (Phase 2+) (GSM); Universal Mobile Telecommunication System (UMTS); Multimedia Messaging Service (MMS); Media formats and codes (3GPP 26.140 version 5.0.0 Release 5).
- a27. ETSI TS 123 140 (v.4.6.0) (2002-03) Digital cellular telecommunication system (Phase 2+) (GSM); Universal Mobile Telecommunication System (UMTS); Multimedia Messaging Service (MMS); Functional description; Stage 2 (3GPP 23.140 version 4.6.0 Release 4).
- a28. OMA-WAP-MMS-ARCH-v1\_1-20021101-c Open Mobile Alliance. Multimedia Messaging Service. Architecture Overview. Version 1.1.
- a29. RFC821 - Simple Mail Transfer Protocol. Postel, J., August 1982.
- a30. RFC2633 - S/MIME Version 3 Message Specification. June 1999.
- a31. WAP-206-MMSCTR -20020115-a. MMS Client Transactions.
- a32. WAP-248-UAPProf-20011020-a. WAP UAPProf.
- a33. WAP-209 MMSEncapsulation -20020105-a. MMS Encapsulation Protocol.
- a34. WAP-183 - ProvCont -20010724-a. Provisioning Content (с учетом Specification Information Note WAP-183-004 - ProvCont -20011025-a).
- a35. WAP-266 - WTA-20010908-a. WAP Wireless Telephony Application.
- a36. WAP-268 - WTAI-20010908-a. WAP Wireless Telephony Application Interface.
- a37. WAP-255 - WTAIGSM-20010908-a. WAP Wireless Telephony Application Interface. GSM Specific Addendum.
- a38. WAP-269 - WTAIIS136-20010908. WAP Wireless Telephony Application Interface. ANSI136 Specific Addendum.
- a39. WAP-234 - SYNC -20010530-a. WAP Sync Spec. Data Synchronisation Specification.
- a40. SyncML Sync Protocol, version 1.0, December 7, 2000.
- a41. SyncML HTTP Binding, version 1.0, December 7, 2000.
- a42. SyncML over WSP, Version 1.0, December 7, 2000.
- a43. РД 45.038-99 «Технические требования к аппаратуре связи, реализующей функции маршрутизации пакетов протокола межсетевого обмена (аппаратура маршрутизации пакетов IP)», утвержденный Госкомсвязи России 06.08.1998г.

## ПРИЛОЖЕНИЕ Б

## Термины и сокращения

CO	Cache Operation – сообщение передаваемое в быстродействующую буферную память с целью аннулирования её содержания
IWF	Interworking function – функциональный объект сопряжения с внешней сетью
HTTP	HyperText Transfer Protocol - протокол передачи гипертекстовых данных
MAC	Message Authentication Code – код аутентификации сообщения
PAP	Push Access Protocol – протокол доступа для технологии push
PKI	Public Key Infrastructure – средства поддержки режима с общим ключом для аутентификации
QOS	Quality Of Service – качество обслуживания
SI	Service Indicator – индикация услуги, которую следует активизировать в качестве реакции на внешнее воздействие
SL	Service Load – активизация услуги без вмешательства пользователя
SMS	Short Message Service – услуга передачи коротких сообщений
TCP/IP	Transmission Control Protocol/Internet Protocol – протокол контроля передачи сообщений/ протокол сети Интернет
TPI	TransPort information Item – заголовок информации транспортного уровня
UCS	Universal multiple-octet coded Character Set – универсальная многооктетная кодированная символьная группа
URL	Universal Resource Locator – универсальный идентификатор ресурсов
USSD	Unstructured Supplementary Service Data – данные неструктурированной вспомогательной услуги
UTF	Unicode Transformation Format – формат трансформации Unicode
WAE	Wireless Application Environment - прикладная среда беспроводной связи
WAP	Wireless Application Protocol - протокол беспроводных приложений
WBMP	Wireless BitMaP - формат побитного отображения для беспроводной связи
WBXML	Wireless Binary XML – двоичный расширяемый язык разметок для беспроводной связи
WCMP	Wireless Control Message Protocol – протокол сообщений управления для беспроводной связи
WDP	Wireless Datagram Protocol - протокол датаграмм для беспроводной связи
WML	Wireless Markup Language - язык разметки для беспроводной связи
WSP	Wireless Session Protocol - сеансовый протокол для беспроводной связи
WTA	Wireless Telephony Application - прикладная услуга беспроводной телефонии
XML	eXensible Markup Language – расширяемый язык разметок