МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.530

Поправка 1
(07/2003)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Процедуры мобильности и совместной работы – Безопасность для мобильных мультимедийных систем и служб

Симметричные процедуры безопасности для мобильности H.323 в H.510

Поправка 1

Рекомендация МСЭ-Т H.530 (2002) – Поправка 1

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ СЛУЖБ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	H.230–H.239
Процедуры связи	H.240–H.259
Кодирование подвижных видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
СИСТЕМЫ И ОКОНЕЧНОЕ ОБОРУДОВАНИЕ ДЛЯ АУДИОВИЗУАЛЬНЫХ СЛУЖБ	H.300–H.399
ДОПОЛНИТЕЛЬНЫЕ УСЛУГИ ДЛЯ МУЛЬТИМЕДИЙНЫХ СЛУЖБ	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и служб серии H	H.510–H.519
Приложения и службы мобильной мультимедийной совместной работы	H.520–H.529
Безопасность для мобильных мультимедийных систем и служб	**H.530–H.539**
Безопасность для приложений и служб мобильной мультимедийной совместной работы	H.540–H.549
Процедуры мобильного взаимодействия	H.550–H.559
Процедуры взаимодействия мобильной мультимедийной совместной работы	H.560–H.569
ШИРОКОПОЛОСНЫЕ МУЛЬТИМЕДИЙНЫЕ СЛУЖБЫ И МУЛЬТИМЕДИЙНЫЕ СЛУЖБЫ В РЕЖИМЕ TRIPLE-PLAY	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т H.530

Симметричные процедуры безопасности для мобильности H.323 в H.510

Поправка 1

Резюме

Настоящая Поправка устраняет один из недостатков в области безопасности, выявленный в Рекомендации МСЭ-Т H.530 (2002/03), который связан с тем, что V-GK не может проверить, является ли сообщение AuthenticationConfirmation (подтверждения аутентификации) свежим. Этот недостаток, таким образом, допускает возможность атак с воспроизведением или атак с подменой (маскарад). Недостаток был устранен путем введения дополнительных параметров безопасности (т. е. параметра W) в сообщение ответа при распределении ключей.

Источник

Поправка 1 к Рекомендации МСЭ-Т H.530 (2002) утверждена 16-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) 14 июля 2003 года в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соответствие положениям данной Рекомендации является добровольным делом. Однако в Рекомендации могут содержаться определенные обязательные положения (для обеспечения, например, возможности взаимодействия или применимости), и тогда соответствие данной Рекомендации достигается в том случае, если выполняются все эти обязательные положения. Для выражения требований используются слова "shall" ("должен", "обязан") или некоторые другие обязывающие термины, такие как "must" ("должен"), а также их отрицательные эквиваленты. Использование таких слов не предполагает, что соответствие данной Рекомендации требуется от каждой стороны.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т H.530

Симметричные процедуры безопасности для мобильности H.323 в H.510

Поправка 1

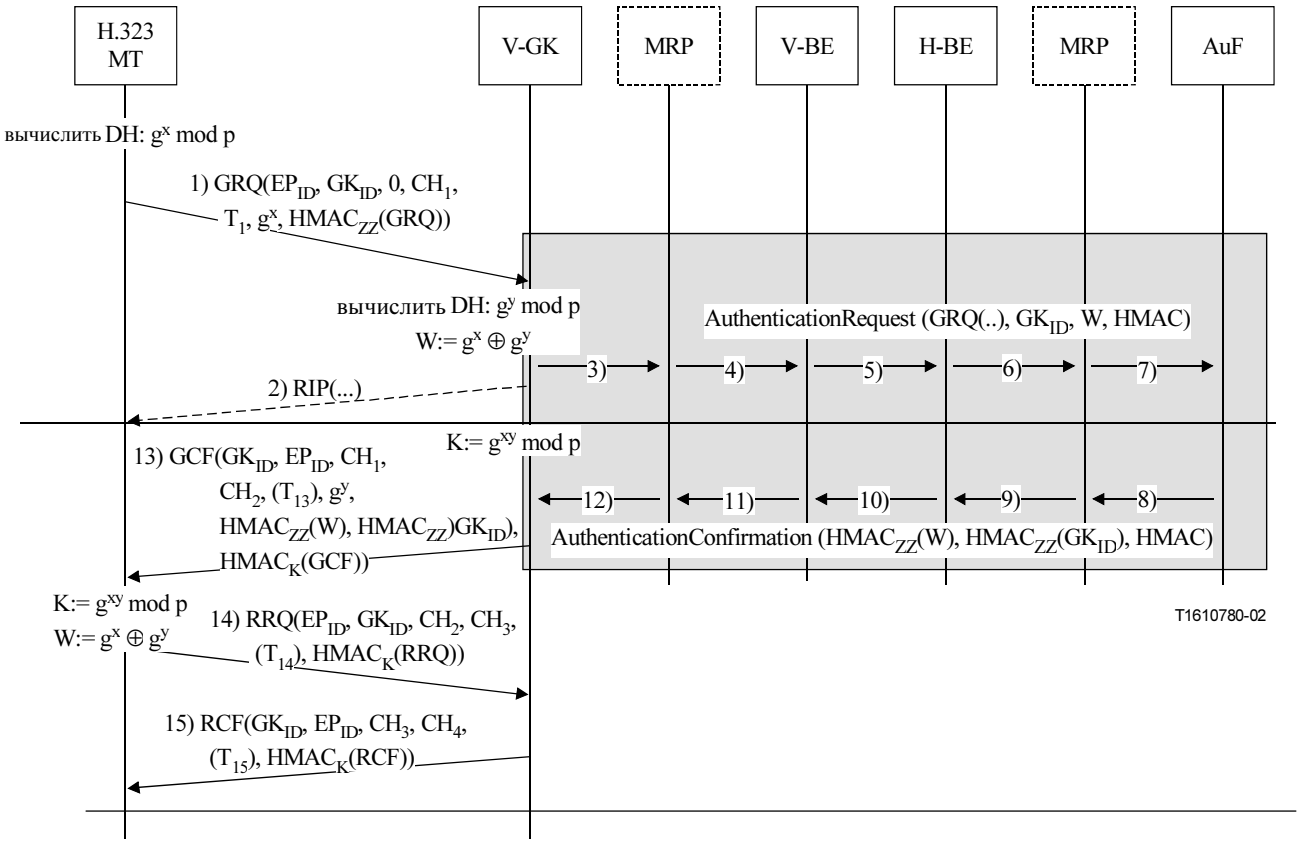
1) Пункт 6, Ссылки

Добавить следующую новую ссылку [8] и обновить все ссылки на [8] и [9] ссылками на [9] и [10], соответственно:

[8] ITU-T Recommendation H.235 (2003), *Security and encryption for H.series (H.323 and other H.245-based) multimedia terminals*.

2) Пункт 8.2

a) Заменить рисунок 2:



следующим рисунком:

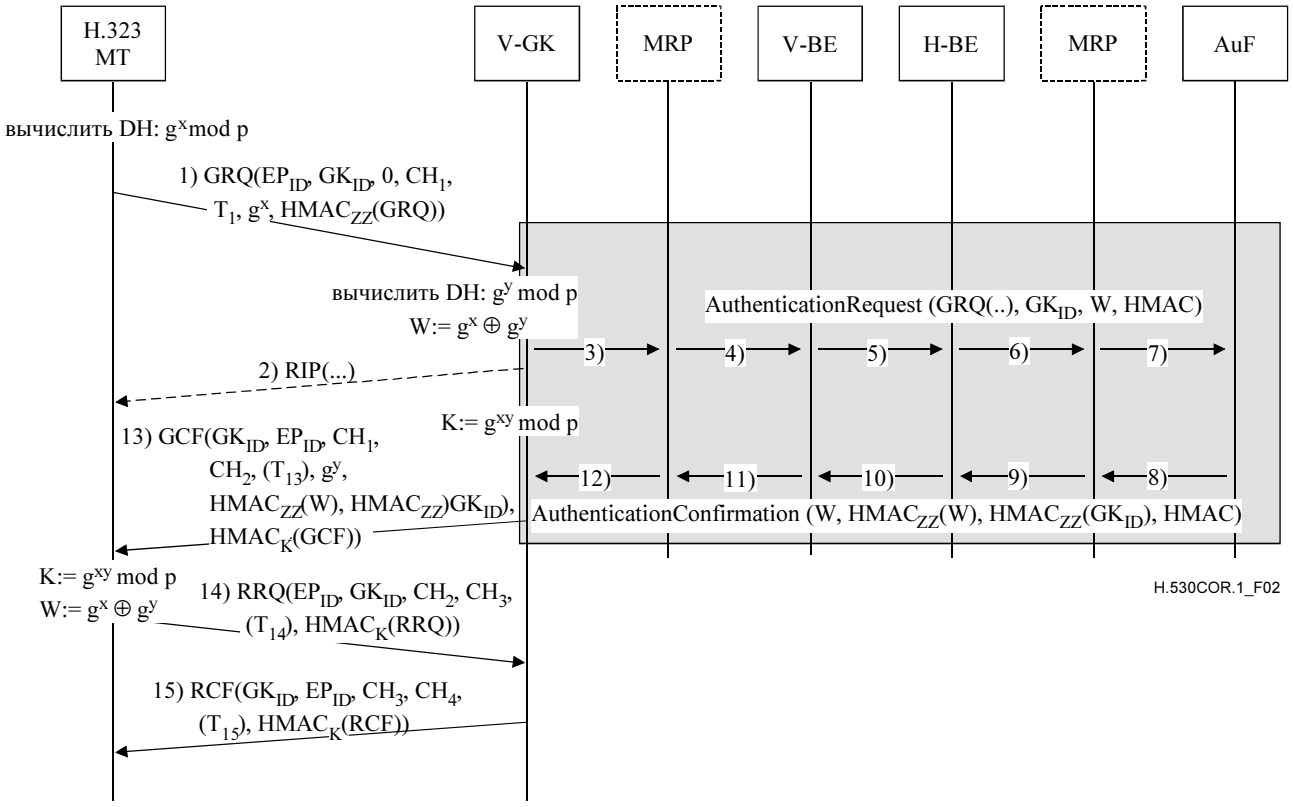
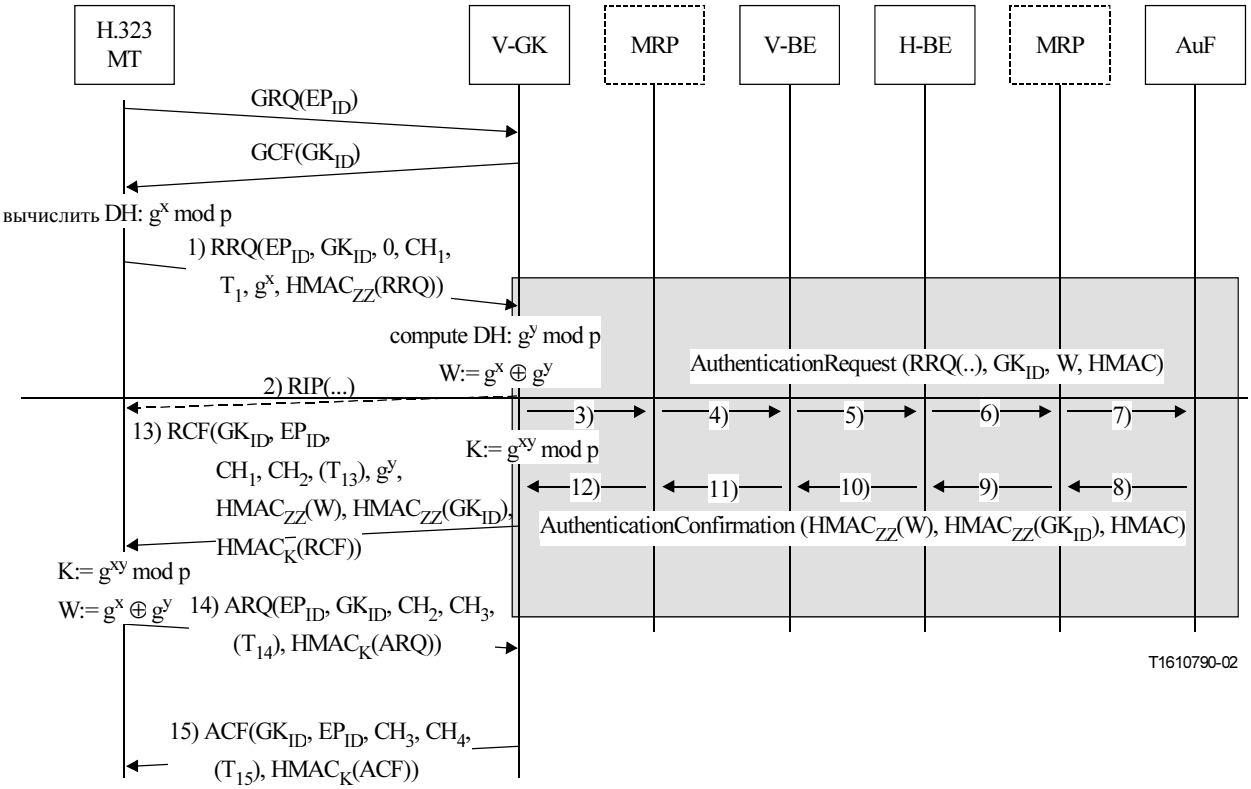


Рисунок 2/H.530 – Аутентификация и распределение ключей на фазе обнаружения GK

b) Заменить рисунок 3:



на:

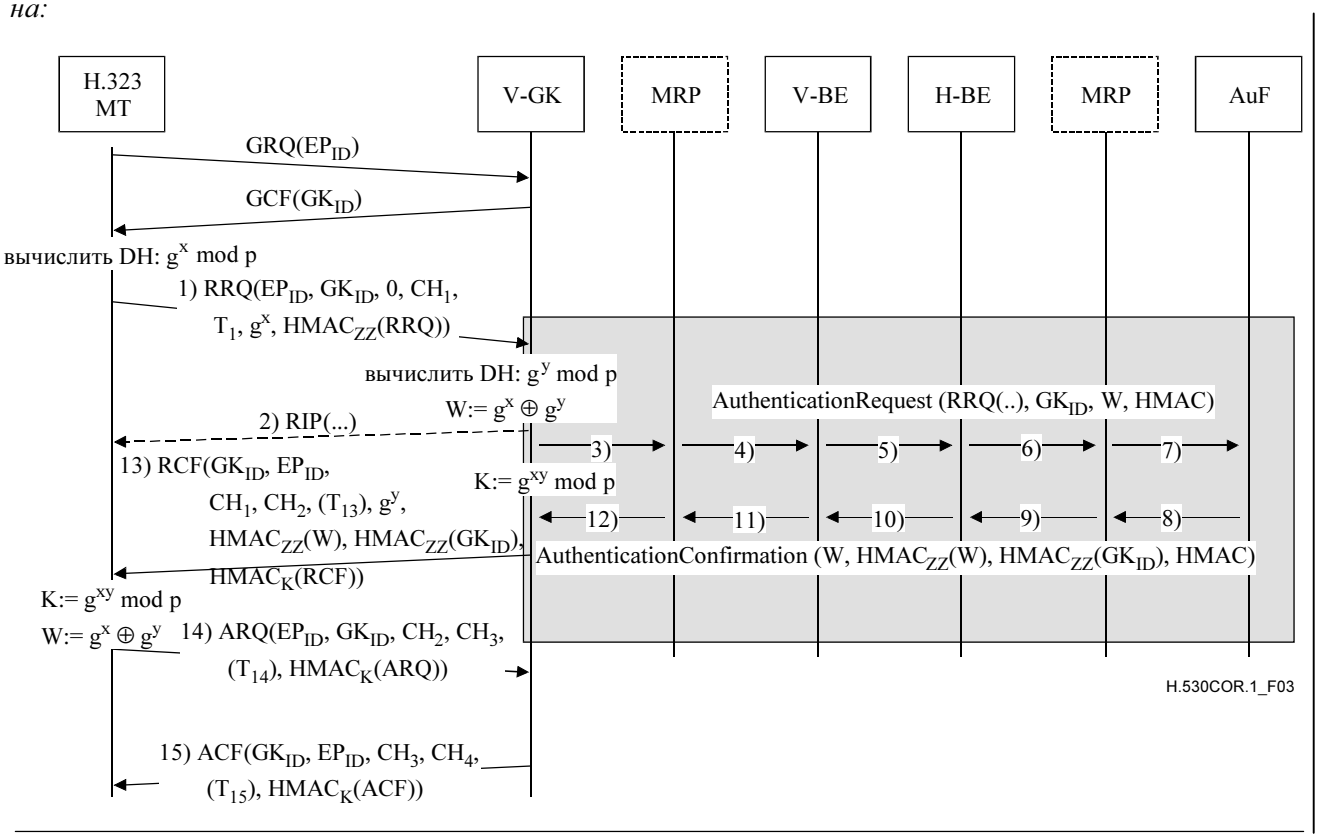


Рисунок 3/H.530 – Аутентификация и распределение ключей на фазе регистрации

3) Пункт 8.2.1

Добавить следующий текст:

…

8.2.1 MT в V-GK

…

Пока **RCF** представляется как сообщение 13), V-GK имеет время для вычисления динамической ссылки *K* с использованием половины ключа Диффи–Хеллмана MT и собственного секретного ключа *y*. Для защиты целостности сообщений HMAC-SHA1-96 в отношении сообщений H.225.0 RAS [1] 96 самых левых битов должны браться из результирующего общего секретного ключа Диффи–Хеллмана, как представлено в последовательности байтов в сети.

V-GK получает **AuthenticationConfirmation/AuthenticationRejection** (подтверждение аутентификации/ отклонение аутентификации) с результатом аутентификации и проверки авторизации по AuF и переданным полномочиям (credentials); см. сообщение 12). V-GK должен проверить, что переданный признак очистки **ClearToken** мобильности содержит то же значение *W*, что и значение, переданное в сообщении 3). Несовпадение означает атаку воспроизведения; в этом случае V-GK должен считать аутентификацию MT со стороны AuF неуспешной и ответить сообщением GRJ/RRJ с **причиной** (reason), установленной равной securityDenial (отказ по защите), или с другим соответствующим кодом ошибки безопасности согласно п. B.2.2 H.235 [8].

V-GK может контролировать получение сообщений **AuthenticationConfirmation**/ **AuthenticationRejection,** используя таймер. Длительность таймера должна выбираться достаточно большой, учитывая транзит по сети и обработку AuF. Если таймер истекает, а соответствующий ответ от AuF не получен, то V-GK должен передать незащищенный **RCF**.

V-GK должен генерировать новое требование CH_2 и построить **RCF**. **RCF** должен передать предыдущее требование CH_1 в **пароле**, новое требование CH_2 в **требовании** в **ClearToken** (очистка маркера) внутри **CryptoToken** (маркера шифрования) **RCF**. Этот **ClearToken** должен также

доставить вычисленный полуключ Диффи–Хеллмана V-GK в поле **halfkey** (полуключ) поля **dhkey** в **ClearToken** этого сообщения. Используемое простое число должно быть включено в поле **modsize**, а генератор DH должен быть включен в поле **generator** (генератор) этого **ClearToken**.

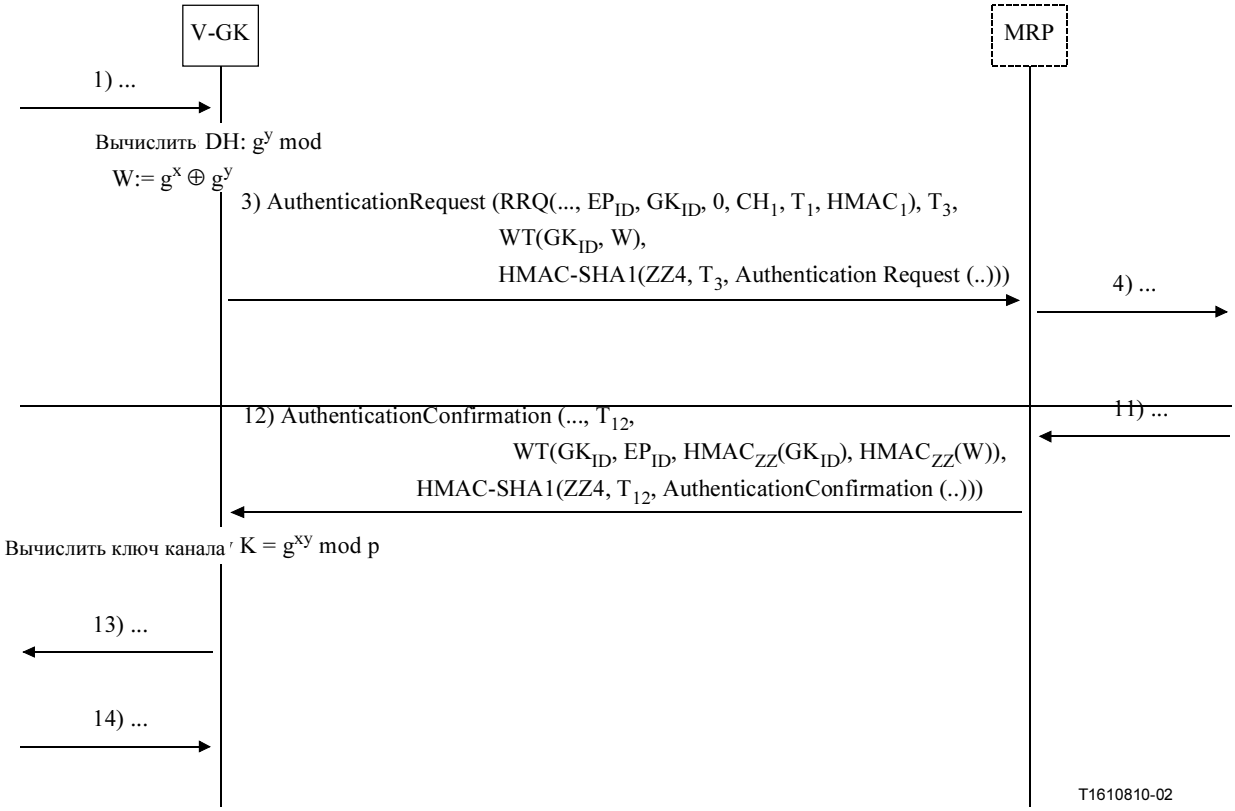
Далее, V-GK должен передать имя пользователя и пароль (полномочия) из AuF в MT. Полномочия включают **ClearToken** мобильности, показанный как **WT()**. Этот **ClearToken** мобильности, с одной стороны, передает аутентифицированное составное значение *W* в поле **halfkey** поля **dhkey**, а с другой – аутентифицированный идентификатор V-GK; значение *W* не должно быть частью переданного **WT()**. Поле **tokenOID** должно быть установлено на "G2", а любые другие параметры в этом **ClearToken** мобильности должны оставаться неиспользованными.

V-GK вычисляет HMAC по всему сообщению **RCF** с использованием ключа для отдельного канала *K*. Таким образом, HMAC служит в качестве ответа на предыдущее требование согласно процедуре I Приложения D/H.235 [4], см. сообщение 13).

…

4) Пункт 8.2.2

Заменить рисунок 5:



на:

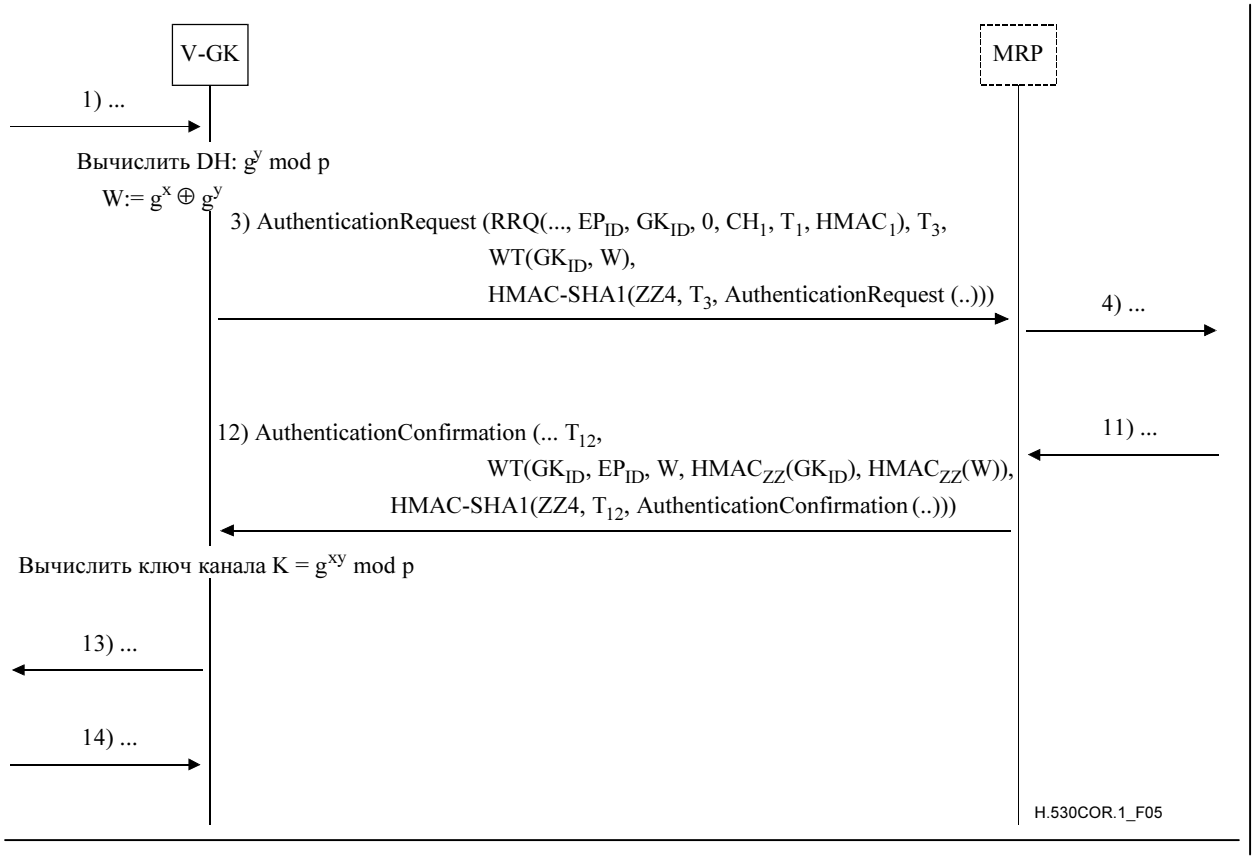
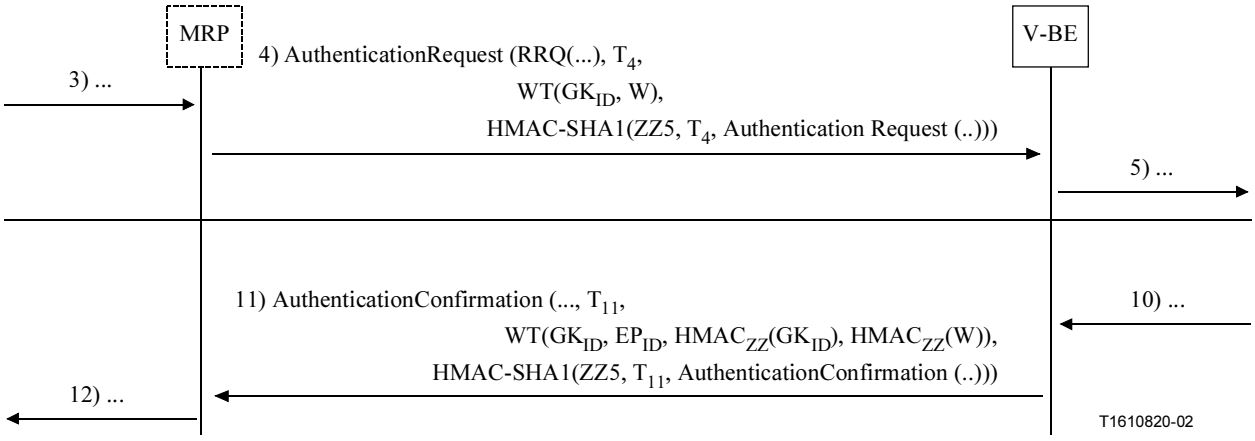


Рисунок 5/H.530 – Передача информации аутентификации между V-GK и MRP

5) Пункт 8.2.3

Заменить рисунок 6:



на:

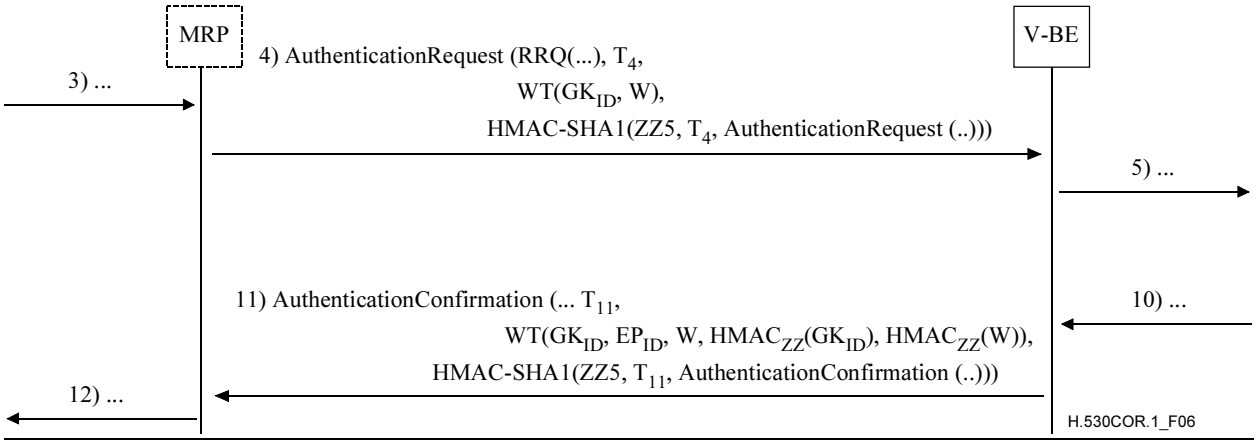
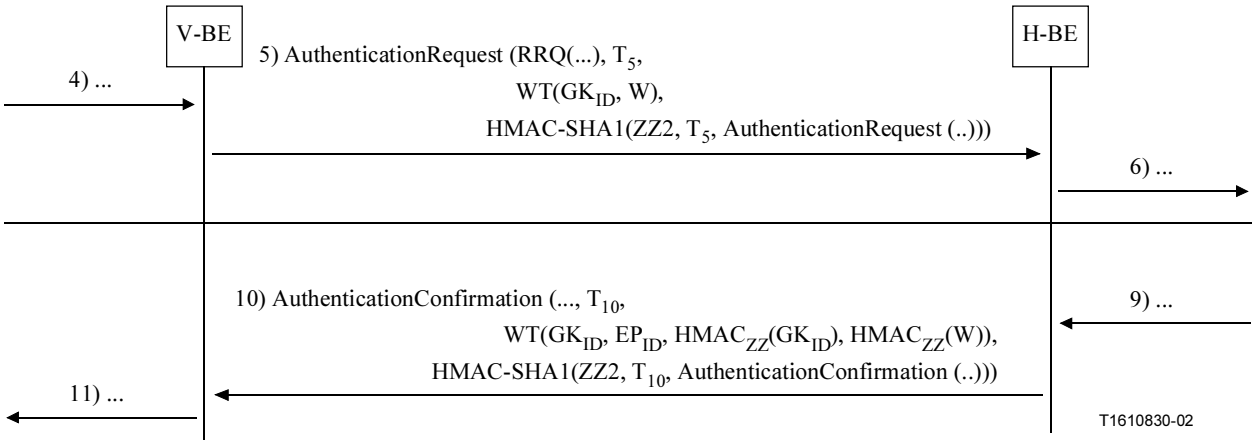


Рисунок 6/H.530 – Передача информации аутентификации между MPR и V-BE

6) Пункт 8.2.4

Заменить рисунок 7:



на:

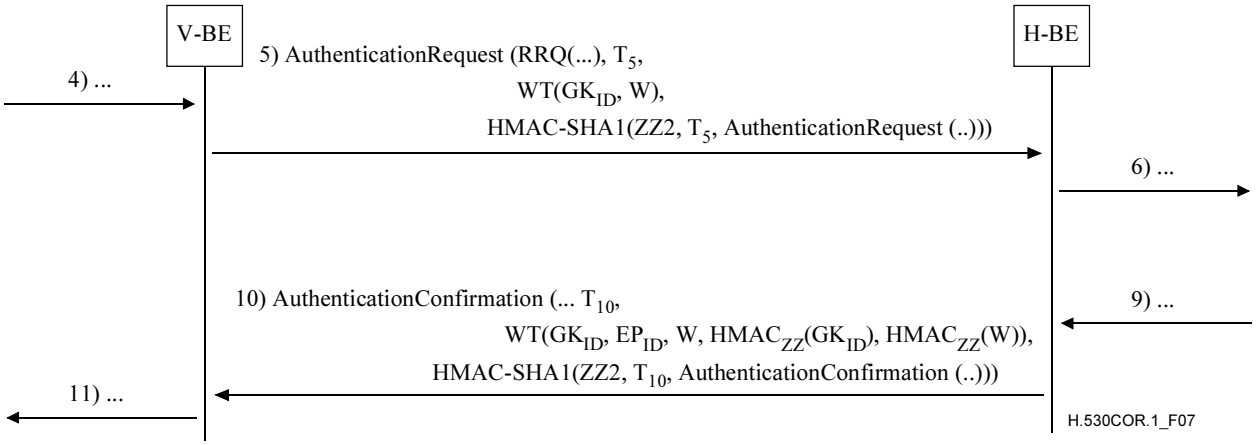
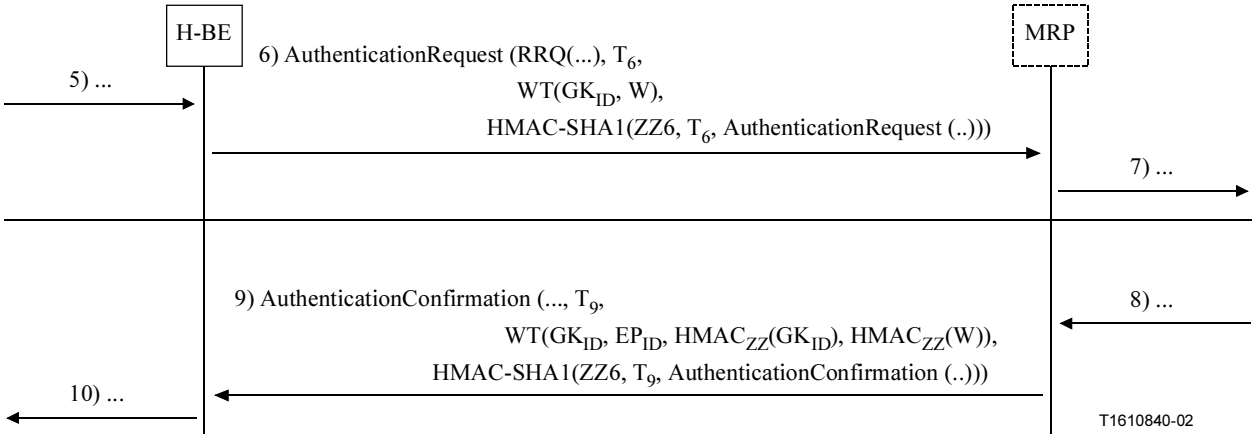


Рисунок 7/H.530 – Передача информации аутентификации между BE

7) Пункт 8.2.5

Заменить рисунок 8:



на:

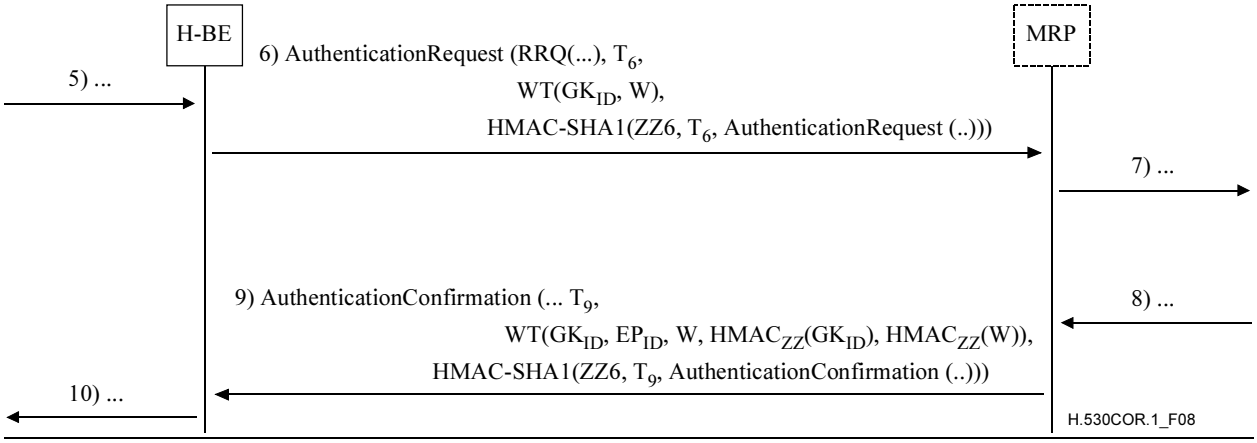
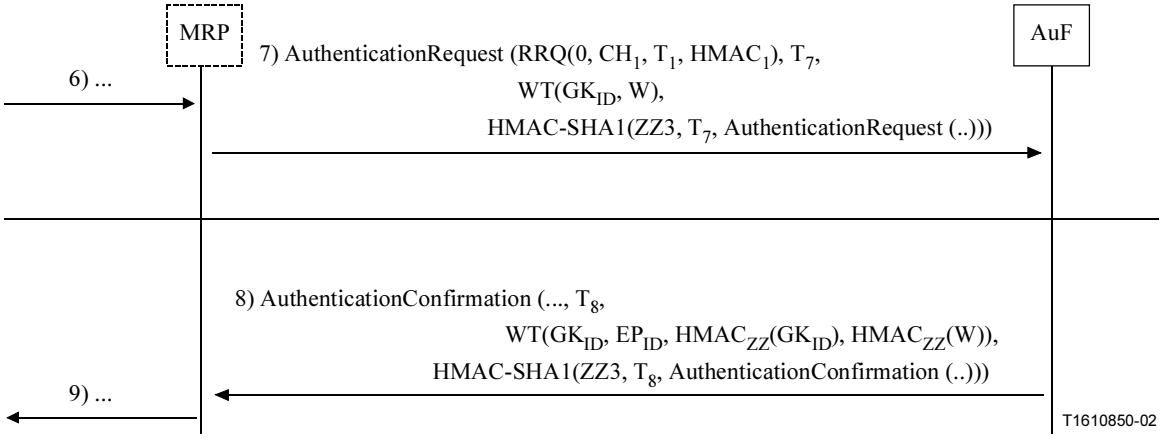


Рисунок 8/H.530 – Передача информации аутентификации между H-BE и MRP

8) Пункт 8.2.6

Заменить рисунок 9:



на:

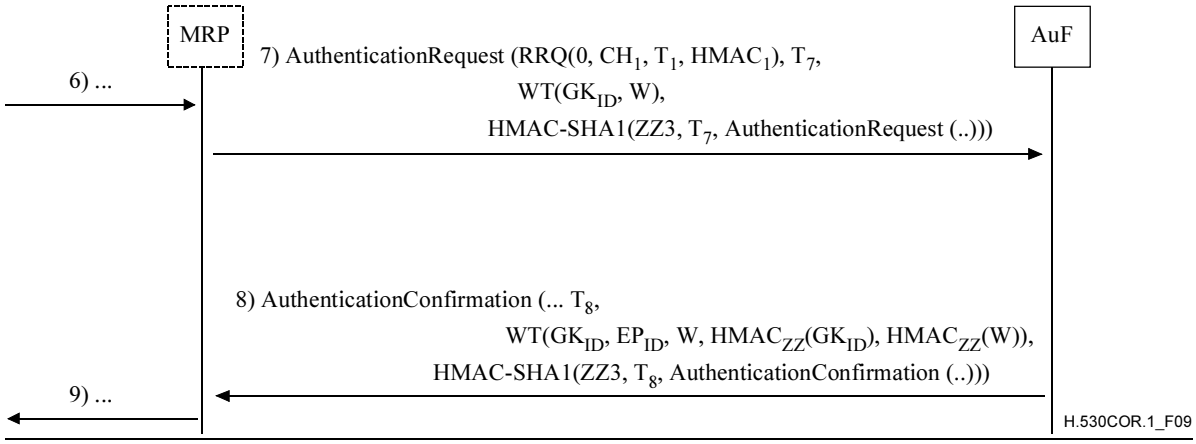


Рисунок 9/H.530 – Передача информации аутентификации между MPR и AuF

9) Пункт 8.2.6

Изменить текст следующим образом:

…

8.2.6 Из MRP в AuF

…

Когда AuF не может применить общий секретный ключ *ZZ*, то следует опустить описанное ниже вычисление аутентифицированных значений полномочий; такой результат не должен быть включен в сообщение **AuthenticationRejection** (отказ в аутентификации). В этом случае **ClearToken** мобильности не присутствует в сообщении **AuthenticationRejection**.

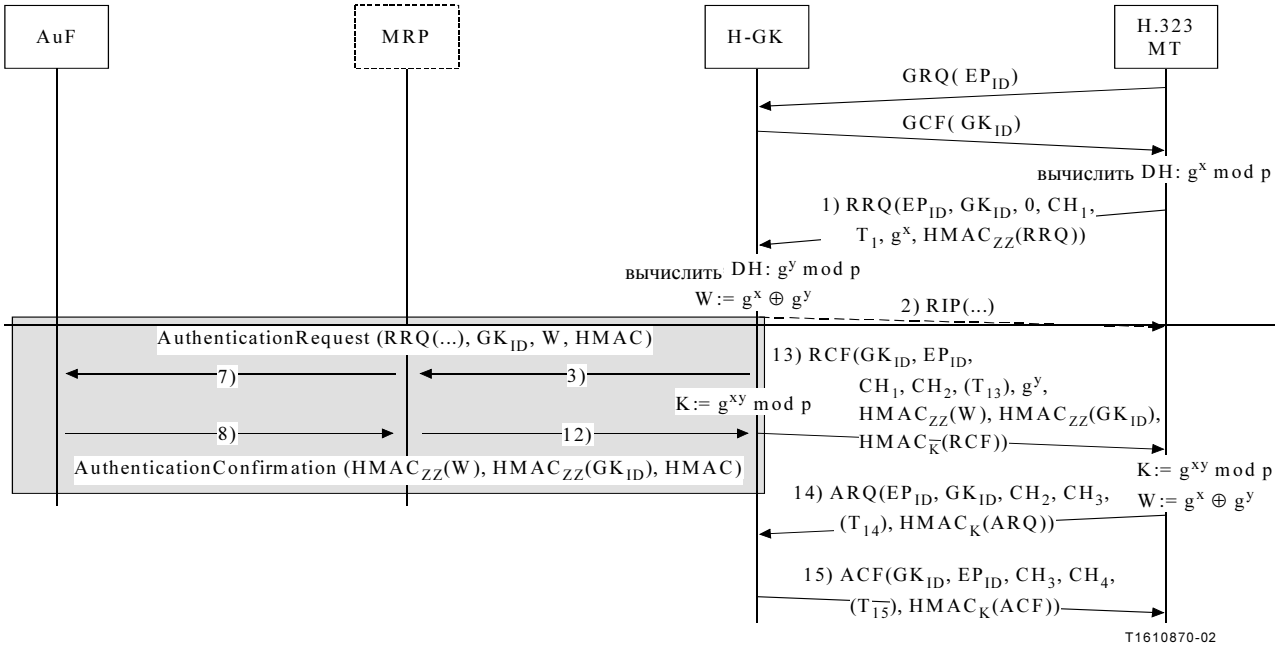
В противном случае AuF должно также вычислить полномочия аутентифицированного составного значения *W*, используя хэш-функцию генерации ключей HMAC-SHA1-96 и *ZZ* в качестве общего стандартного ключа. Аутентифицированное составное значение *W* должно быть включено в отдельный **ClearToken** мобильности, где результат записывается в поле **halfkey** поля **dhkey** в этом **ClearToken** мобильности. Далее, AuF должно вычислить аутентифицированный GK_{ID} как другое полномочие, используя хэш-функцию генерации ключей HMAC-SHA1-96 и *ZZ* в качестве общего стандартного ключа. Результат должен быть включен в поле **generator** (генератор) этого **ClearToken**. AuF также должно включать *W* в поле **modsize dhkey**; это позволяет V-GK распознавать сообщение **AuthenticationConfirmation**/**AuthenticationRejection** как свежее (fresh). Идентификатор **generalID** должен передать GK_{ID}, а **sendersID** – EP_{ID} в этом **ClearToken**. Это позволит V-GK связать сообщение **AuthenticationConfirmation**/**AuthenticationRejection** с соответствующим сообщением **AuthenticationRequest** (запрос аутентификации). Поле **tokenOID** этого **ClearToken** должно быть установлено на "G2", а любые другие параметры в этом **ClearToken** мобильности должны оставаться неиспользованными. **ClearToken** мобильности показан как **WT()**.

Должна использоваться новая метка времени T_8, а ответное сообщение должно быть защищено согласно процедуре I Приложения D/H.235 [4], с использованием общего секретного ключа *ZZ3*; см. сообщение 8).

…

10) Пункт 8.5

Заменить рисунок 11:



на:

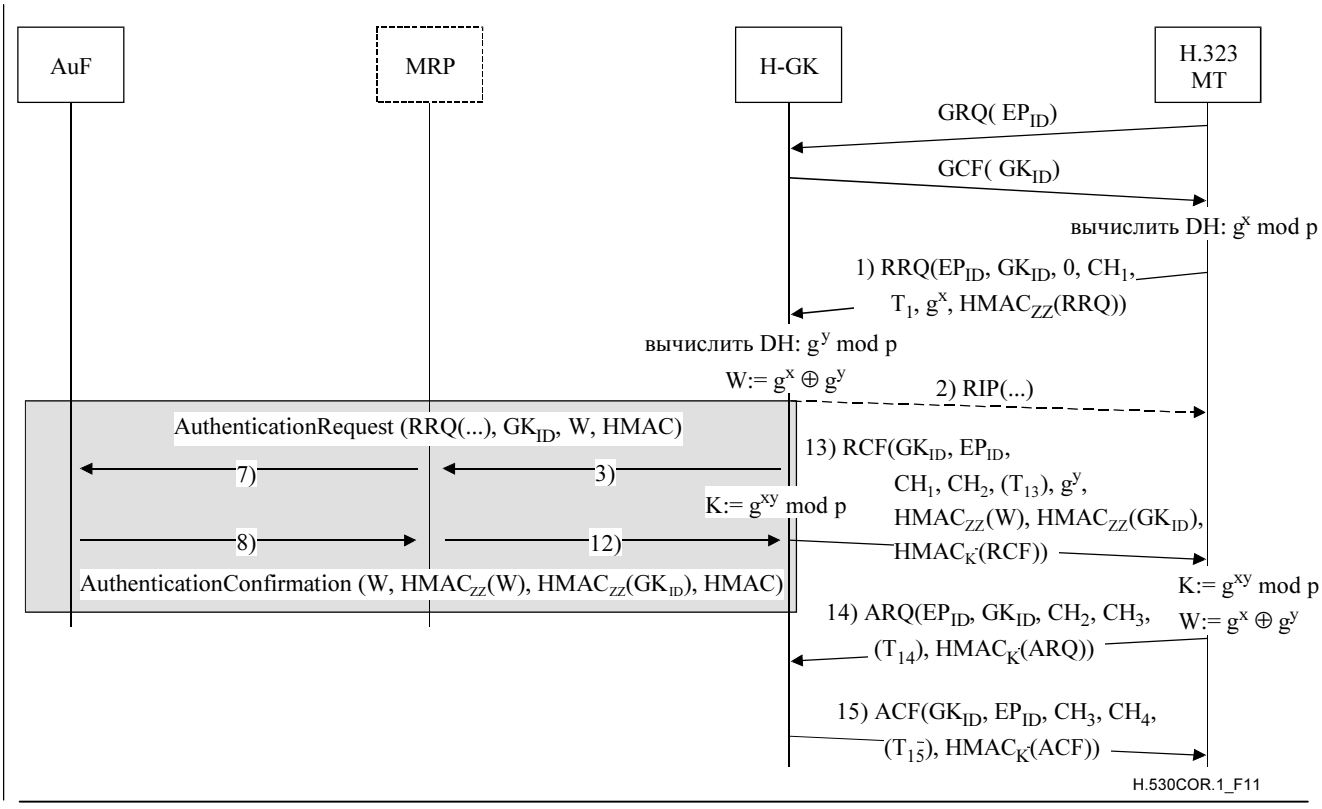


Рисунок 11/H.530 – Аутентификация MT в базовом домене на фазе регистрации

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	**Аудиовизуальные и мультимедийные системы**
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура и аспекты межсетевого протокола (IP)
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2004 г.