Зарегистрировано в Минюсте России 27 июня 2018 г. N 51448

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 13 июня 2018 г. N 275

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПРАВИЛА ПРИМЕНЕНИЯ ОБОРУДОВАНИЯ КОММУТАЦИИ СЕТЕЙ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ. ЧАСТЬ VI. ПРАВИЛА ПРИМЕНЕНИЯ УЗЛОВ СВЯЗИ С ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ АРХИТЕКТУРОЙ СТАНДАРТОВ UMTS И/ИЛИ GSM 900/1800, УТВЕРЖДЕННЫЕ ПРИКАЗОМ МИНИСТЕРСТВА СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 27.06.2011 N 160

В соответствии с пунктами 2 и 2.1 статьи 12 и пунктом 2 статьи 64 Федерального закона от 7 июля 2003 г. N 126-ФЗ "О связи" (Собрание законодательства Российской Федерации, 2003, N 28, ст. 2895; 2006, N 31, ст. 3452; 2010, N 7, ст. 705; 2011, N 45, ст. 6333; 2016, N 28, ст. 4558; 2017, N 31, ст. 4742; 2018, N 17, ст. 2419) приказываю:

1. Утвердить прилагаемые изменения, которые вносятся в Правила применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VI. Правила применения узлов связи с территориально распределенной архитектурой стандартов UMTS и/или GSM 900/1800, утвержденные приказом Министерства связи и массовых коммуникаций Российской Федерации от 27.06.2011 N 160 (зарегистрирован Министерством юстиции Российской Федерации 20 июля 2011 г., регистрационный N 21423), с изменениями, внесенными приказами Министерства связи и массовых коммуникаций Российской Федерации от 01.02.2012 N 30 (зарегистрирован Министерством юстиции Российской Федерации 22 февраля 2012 г., регистрационный N 23316), от 23.04.2013 N 93 (зарегистрирован Министерством юстиции Российской Федерации 14 июня 2013 г., регистрационный N 28788) и от 24.10.2017 N 572 (зарегистрирован Министерством юстиции Российской Федерации 5 февраля 2018 г., регистрационный N 49882).

2. Установить, что настоящий приказ вступает в силу с 1 декабря 2019 г.

3. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Министр
К.Ю.НОСКОВ

Утверждены
приказом Министерства

цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 13.06.2018 N 275

ИЗМЕНЕНИЯ,
КОТОРЫЕ ВНОСЯТСЯ В ПРАВИЛА ПРИМЕНЕНИЯ ОБОРУДОВАНИЯ КОММУТАЦИИ СЕТЕЙ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ. ЧАСТЬ VI. ПРАВИЛА ПРИМЕНЕНИЯ УЗЛОВ СВЯЗИ С ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ АРХИТЕКТУРОЙ СТАНДАРТОВ UMTS И/ИЛИ GSM 900/1800, УТВЕРЖДЕННЫЕ ПРИКАЗОМ МИНИСТЕРСТВА СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 27.06.2011 N 160

1. Подпункт 4 пункта 4 изложить в следующей редакции:

"4) опорного регистра местонахождения и/или центра аутентификации (далее - HLR/AuC);".

2. Пункт 4 дополнить подпунктом 8:

"8) аппаратного модуля безопасности (далее - HSM) (в случае реализации криптографических алгоритмов аутентификации абонентов в отдельном аппаратном модуле безопасности).".

3. Абзац первый пункта 18 изложить в следующей редакции:

"18. Для средств связи, выполняющих функции опорного регистра местонахождения HLR и/или функции центра аутентификации AuC, устанавливаются следующие требования:".

4. Подпункт 2 пункта 3 приложения N 1 дополнить подпунктами "в" и "г":

"в) реализация процедур аутентификации и идентификации абонентов осуществляется с использованием средств криптографической защиты информации, имеющих подтверждение соответствия требованиям по безопасности информации класса KA для оборудования коммутации узлов связи, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

г) в случае реализации криптографических алгоритмов аутентификации и идентификации абонентов в отдельном аппаратном модуле безопасности HSM взаимодействие HLR/AuC с HSM должно осуществляться согласно протоколу, приведенному в приложении N 10.1 к Правилам.".

5. Дополнить приложением N 10.1 в следующей редакции:

"Приложение N 10.1
к Правилам применения
оборудования коммутации сетей
подвижной радиотелефонной
связи. Часть VI. Правила
применения узлов связи
с территориально распределенной
архитектурой стандартов
UMTS и/или GSM 900/1800

ПРОТОКОЛ
ВЗАИМОДЕЙСТВИЯ ОПОРНОГО РЕГИСТРА МЕСТОНАХОЖДЕНИЯ HLR И/ИЛИ ЦЕНТРА АУТЕНТИФИКАЦИИ AUC С ОТДЕЛЬНЫМ АППАРАТНЫМ МОДУЛЕМ БЕЗОПАСНОСТИ HSM, ВЫПОЛНЯЮЩИМ КРИПТОГРАФИЧЕСКИЕ ФУНКЦИИ АУТЕНТИФИКАЦИИ АБОНЕНТОВ

1. Для взаимодействия опорного регистра местонахождения и/или центра аутентификации HLR/AuC с HSM, выполняющих криптографические функции аутентификации абонентов, должны использоваться следующие сообщения:

1) запрос со стороны HLR/AuC аутентификационной информации (Authentication Crypto Request - ACR); в таблице N 1 приведено содержание информационных элементов, используемых в данном сообщении;

Таблица N 1.

Информационный элемент	Содержание информационного элемента
Code	Код сообщения HLR/AuC. Длина: 48 бит.
K	Ключ K, который хранится в HLR/AuC. Длина: 128 бит.
AMF	Поле управления аутентификацией AMF (Authentication management field), предусмотренное пунктом 6.3 ETSI TS 133 102. Длина: 16 бит.
SQN	Порядковый номер SQN (sequence number), предусмотренный пунктом 6.3 ETSI TS 133 102. Длина: 48 бит.
AIR-Filler	Данный информационный элемент обеспечивает превышение длиной запроса длины соответствующего ему ответа. Длина: 448 бит.

2) ответ HSM с аутентификационной информацией (Authentication Crypto Answer - ACA); в таблице N 2 приведено содержание информационных элементов, используемых в данном сообщении;

Таблица N 2.

Информационный элемент	Содержание информационного элемента

Code	Код сообщения HSM. Длина: 48 бит.
Authentication Vector	Вектор аутентификации (AV), предусмотренный пунктом 6.3 ETSI TS 133 102. Длина: 576 бит.

3) запрос со стороны HLR/AuC аутентификационной информации при ресинхронизации (Resynchronization Crypto Request - RCR); в таблице N 3 приведено содержание информационных элементов, используемых в данном сообщении;

Таблица N 3.

Информационный элемент	Содержание информационного элемента
Code	Код сообщения HLR/AuC. Длина: 48 бит.
K	Ключ абонента K, предусмотренный пунктом 6.3 ETSI TS 133 102. Длина: 128 бит.
RAND (Random challenge)	Случайный параметр RAND, предусмотренный пунктом 6.3 ETSI TS 133 102. Длина: 128 бит.
Conc (SQNMS)	Криптографически защищенный случайный порядковый номер Conc (SQN_{MS}), предусмотренный пунктом 6.3 ETSI TS 133 102. Длина: 48 бит.

4) ответ HSM с аутентификационной информацией при ресинхронизации (Resynchronization Crypto Answer - RCA); в таблице N 4 приведено содержание информационных элементов, используемых в данном сообщении.

Таблица N 4.

Информационный элемент	Содержание информационного элемента
Code	Код сообщения HSM. Длина: 48 бит.
XMACS	Криптографически защищенная имитовставка XMACS, предусмотренная пунктом 6.3 ETSI TS 133 102.

	Длина: 64 бит.
SQNMS	Порядковый номер SQN_{MS}, предусмотренный пунктом 6.3 ETSI TS 133 102. Длина: 48 бит.

2. HLR/AuC при реализации протокола взаимодействия с HSM должен обеспечить:

1) отправку в HSM запроса для генерации данных аутентификации;

2) установку для каждого отправленного запроса уникального адреса отправителя сообщения согласно протоколу взаимодействия 4 уровня (транспортного протокола передачи дейтаграмм пользователя - UDP);

3) ожидание для каждого отправленного запроса ответа от HSM в течение установленного при настройке времени.

3. HSM при реализации протокола взаимодействия с HLR/AuC должен обеспечить:

1) принятие от HLR/AuC корректного запроса для генерации данных аутентификации, обработку запроса и передачу ответа в HLR/AuC;

2) совпадение указанного в ответе адреса получателя сообщения с адресом, указанным в запросе отправителя сообщения, согласно протоколу взаимодействия 4 уровня;

3) отказ в ответе при поступлении от HLR/AuC некорректных запросов;

4) оповещение системы об отказе в ответе путем отключения интерфейса на физическом уровне взаимодействия.

4. Реализация протокола взаимодействия 4 уровня должна осуществляться с учетом следующих требований:

1) для адресации запросов и ответов согласно протоколу взаимодействия 4 уровня должны использоваться UDP-порты из диапазона 49152 - 65535;

2) адреса получателя ответов и отправителя ответов согласно протоколу взаимодействия 4 уровня должны устанавливаться одинаковыми в конфигурациях HLR/AuC и HSM соответственно;

3) информация, передаваемая в сообщениях согласно протоколу взаимодействия 4 уровня, должна быть защищена от несанкционированного доступа к ней.

5. Значения кодов информационных сообщений при взаимодействии HLR/AuC с HSM должны соответствовать значениям, приведенным в таблице N 5.

Таблица N 5.

	Информационное сообщение	Сокращение	Значение кода/Code
1.1	Authentication Crypto Request без использования AK	ACR	0
1.2	Authentication Crypto Request с использованием AK	ACR	1
2.	Authentication Crypto Answer	ACA	2

3.1	Resynchronization Crypto Request без использования AK	RCR	4
3.2	Resynchronization Crypto Request с использованием AK	RCR	5
4.	Resynchronization Crypto Answer	RCA	6

"

6. Приложение 11 дополнить пунктами 64 и 65 в следующей редакции:

"64. ETSI TS - European Telecommunications Standard Institute Technical Specification (техническая спецификация Европейского института по стандартизации в области телекоммуникаций).

65. HSM - Hardware Security Module (аппаратный модуль безопасности).".