TIA STANDARD

Project 25

Digital Land Mobile Radio Link Layer Authentication

TIA-102.AACE-A **April 2011**

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

tiaonline.org

NOTICE

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. The existence of such Standards and Publications shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such Standards and Publications. Neither shall the existence of such Standards and Publications preclude their voluntary use by Non-TIA members, either domestically or internationally.

Standards and Publications are adopted by TIA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(From Project No. 3-0206-RV1-1, formulated under the cognizance of the TIA TR-8 Mobile and Personal Private Radio Standards, TR-8.3 Subcommittee on Encryption Subcommittee).

Published by
©TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Standards and Technology Department
2500 Wilson Boulevard
Arlington, VA 22201 U.S.A.

PRICE: Please refer to current Catalog of
TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS AND ENGINEERING PUBLICATIONS
or call IHS, USA and Canada
(1-877-413-5187) International (303-397-2896)
or search online at http://www.tiaonline.org/standards/catalog/

NOTICE OF COPYRIGHT

This document is copyrighted by the TIA.

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Engineering Manual ("Manual"), the current and predecessor versions of which are available at http://www.tiaonline.org/standards/procedures/manuals/TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). TIA does not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA disclaims any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or any editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. TIA makes no search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. TIA takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. TIA will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

If the Document contains one or more Normative References to a document published by another organization ("other SSO") engaged in the formulation, development or publication of standards (whether designated as a standard, specification, recommendation or otherwise), whether such reference consists of mandatory, alternate or optional elements (as defined in the TIA Engineering Manual, 4th edition) then (i) TIA disclaims any duty or obligation to search or investigate the records of any other SSO for IPR or letters of assurance relating to any such Normative Reference; (ii) TIA's policy of encouragement of voluntary disclosure (see Engineering Manual Section 6.5.1) of Essential Patent(s) and published pending patent applications shall apply; and (iii) Information as to claims of IPR in the records or publications of the other SSO shall not constitute identification to TIA of a claim of Essential Patent(s) or published pending patent applications.

TIA does not enforce or monitor compliance with the contents of the Document. TIA does not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NONINFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTNTS.

TIA SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

Contents

List of Figures

List of Tables

Foreword

(This foreword is not part of this document.)

This document has been submitted to APCO/NASTD/FED by the Telecommunications Industry Association (TIA), as provided for in a Memorandum of Understanding (MOU) dated December, 1993. That MOU provides that APCO/NASTD/FED will devise a Common System Standard for digital public safety communications (the Standard), and that TIA shall provide technical assistance in the development of documentation for the Standard.

This document has been developed by TR8.3 (Encryption) with inputs from the APCO Project 25 Interface Committee (APIC), the APIC Encryption Task Group, and TIA Industry members.

This document is being published to provide technical information on the emerging digital techniques for Land Mobile Radio Service.

Patent Identification

The reader's attention is called to the possibility that compliance with this document may require the use of one or more inventions covered by patent rights.

By publication of this document no position is taken with respect to the validity of those claims or any patent rights in connection therewith. The patent holders so far identified have, we believe, filed statements of willingness to grant licenses under those rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such licenses.

The following patent holders and patents have been identified in accordance with the TIA intellectual property rights policy:

No patents have been identified.

TIA shall not be responsible for identifying patents for which licenses may be required by this document or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

1 INTRODUCTION

Authentication of subscriber units is a vital component of a general land mobile radio system. The purpose of this document is to define a Challenge and Response Authentication method for use on trunked radio systems.

1.1 Scope

The authentication service described in this document is applicable to FDMA and TDMA trunking systems using an FDMA trunking control channel. Authentication is a supplementary service for trunked radio systems. This document describes two forms of authentication: unit authentication and mutual authentication. If unit authentication is implemented it shall be implemented as specified herein. If mutual authentication is implemented , it shall be implemented as specified herein.

This document defines the full standard across the U_m interface.

1.2 Document Description

This document describes Challenge and Response Authentication designed to protect the family of Project 25 systems.

- Section 1 provides a general description, definitions and abbreviations.
- Section 2 provides high-level information about Challenge and Response Authentication.
- Section 3 provides procedures and operational descriptions.
- Section 4 provides a listing of control channel messages
- Section 5 provides information on key management and provisioning.
- Section 6 provides algorithm details.

1.3 Document Revision History

Revision date	Revision comments
July 31, 2003	Initial version
October 10, 2003	Revision 2, updated document to fill in missing sections.
March 11, 2004	Revision 3, add ISSI and Intra-RFSS Key Management, added infrastructure failure to get RS KS rule, and added that K should be store in non-volatile memory.
June 11, 2004	Revision 4, removed Pre-Defined Roaming. Moved ISSI, Intra-RFSS, and to Security Services Architecture document. Moved Provisioning File Format to Security Services Provisioning document. Added that the interface between SU and Provisioning will be specified by the Key Fill standard. Added example state diagrams for authentication that also provides context for error cases.
August 4, 2004	Revision 5, updated based on NCS and M/A-COM comments.
September 16, 2004	Revision 6, updated based on September 13, 2004 Encryption Task Group meeting.
January 31, 2005	Revision 7, added MSC for subscriber initiated authentication demand, modified message returned from the RFSS on authentication failure and fixed typographic errors.
March 8, 2005	Revision 8, fixed typographic errors, corrected AM2 and AM4 sample data, segmented out informative references and removed Annex A Control Channel Messages.
May 11, 2005	PN-3-0206, Ballot Version
September 9, 2005	TIA 102.AACE, released for publication
February 25, 2010	Proposed edits for Standalone authentication

1.4 Definitions

Advanced Encryption Standard (AES) - A standardized cryptographic algorithm to replace the Data Encryption Standard (DES). AES has a 128 block size and AES-128 indicates that a 128 bit key is used with AES as described in reference [2].

Adversary FNE – A FNE that is not a valid FNE.

Adversary SU – A SU that is not a valid SU.

Authenticated SU – A SU whose SUID has passed a challenge and response authentication. This SU has proven that it is the valid SU.

Authentication – The process to prove that a SU is valid.

Authentication Facility (AF) – A functional process within the FNE. It is being included in order to show the specialized functions that the FNE must implement in order to support authentication. Such functions include assignment of K to SUID, generation of KS and KS' using RS to allow the RFSS to perform authentication, and providing confidentiality of K within the FNE.

Authentication Key (K) – A secret symmetric key needed to prove authenticity.

Authorized SU – A SU whose SUID is programmed into the system. An authorized SU may be required to authenticate to prove it is the valid SU.

Challenge and Response Authentication – An authentication process in which a source sends a challenge to a target and the target sends a response based on the challenge and a secret held between the target and source.

Fixed Network Equipment (FNE) – The AF and RFSS.

K Provisioning System – A system that delivers K to the SU and AF. The provisioning system can create K or may acquire K from a Secure Authority. The provisioning system may have a secure repository for K before it is transferred to the AF.

Mutual Authentication – A process to prove that the SU is valid to the FNE, along with the FNE proving it is valid to the SU. An interlaced challenge and response authentication is done.

RF Sub-System (RFSS) - An RFSS consists of one or more sites.

Secure Authority – A trusted source of key material to be used as K.

Site - A site consists of one or more channels.

Standalone Authentication – An authentication outside of registration.

Subscriber Unit Identity (SUID) – A 56-bit identity that uniquely identifies a subscriber. It consists of the WACN, System ID and Subscriber ID.

Subscriber ID – A 24-bit unit identity portion of the subscriber unit identity. This field along with the WACN ID and System ID uniquely identify a subscriber unit.

SUID Provisioning System – A system that delivers the SUID to the SU and receives the SN from the SU. The system gives the SUID-SN pair to the RFSS so the RFSS can send the SUID-SN pair to the AF.

System ID – A 12-bit ID to identify the system.

Valid FNE – A FNE that is not an impostor.

Valid SU – A SU that is not an impostor.

Wide Area Communication Network ID (WACN) – A 20-bit ID to define the network address

1.5 Abbreviations

AES	Advanced Encryption Standard
AES-128	AES using a 128 bit key
AF	Authentication Facility
AM1	Authentication Mechanism 1
AM2	Authentication Mechanism 2
AM3	Authentication Mechanism 3
AM4	Authentication Mechanism 4
ECB	Electronic Codebook
ESN	Electronic Serial Number
FNE	Fixed Network Equipment
ISP	Inbound Signaling Packet
K	Authentication Key
KMF	Key Management Facility
KS	Session Authentication Key
KS'	Mutual Session Authentication Key
MFID	Manufacture's Identity
MSC	Message Sequence Chart
OSP	Outbound Signaling Packet
OTAR	Over-The-Air Rekeying
R1	Result 1
R2	Result 2
RAND1	Random Challenge 1
RAND2	Random Challenge 2
RES1	Response1
RES2	Response 2
RFSS	RF Sub-System
RS	Random Seed
S	Standalone
SN	Serial Number
SU	Subscriber Unit
SUID	Subscriber Unit Identity
WACN	Wide Area Communication Network
XRES1	Expected Response 1
XRES2	Expected Response 2

1.6 References

The following documents contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

1.6.1 Normative References

[1] *Project 25 Trunking Control Channel Messages*, TIA/EIA-102.AABC, April 2004
[2] *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001
[3] *Recommendation for Block Cipher Modes of Operation,* National Institute of Standards and Technology Special Publication 800-38A, 2001 Edition
[4]

1.6.2 Informative References

[5] *Key Fill Device (KFD)Interface Protocol,* TIA-102.AACD,February 2005
[6] *Project 25 Over-The-Air-Rekeying (OTAR) Protocol,* TIA-102.AACA, April 2001

1.7 Overview

The authentication defined in this document is designed to provide a desired degree of interoperation. Authentication will typically require an additional allocation of resources. This expense could be in terms of channel capacity, development complexity, equipment complexity, administration, maintenance, etc.

The authentication technique described in this document is Challenge and Response Authentication. It is a well-known and broadly used authentication technique.

2 AUTHENTICATION

Authentication is the process of ensuring a Subscriber Unit (SU) is a valid unit. Mutual authentication is the process of ensuring a SU and Fixed Network Equipment (FNE) are both valid, which allows the SU to validate the FNE. Authentication can be performed with an authorized SU that has been provisioned for authentication.

A challenge and response authentication is used for authentication and mutual authentication. A secret symmetric key called the Authentication Key, K, is held in common using non-volatile memory in the SU and FNE order to authenticate the SU and optionally authenticate the FNE. Each SU has its own individual K which is associated with the SU programmed Subscriber Unit Identity (SUID). When there are multiple SUID in a SU, the SU will have a K per SUID. When the FNE authenticates the SU, the FNE sends a challenge to the SU, and the SU returns a response that requires knowledge of K. The SU can authenticate the FNE by making authentication mutual. With mutual authentication, the SU also challenges the FNE and the FNE returns a response that requires knowledge of K.

2.1 Challenge and Response Authentication Block Diagram

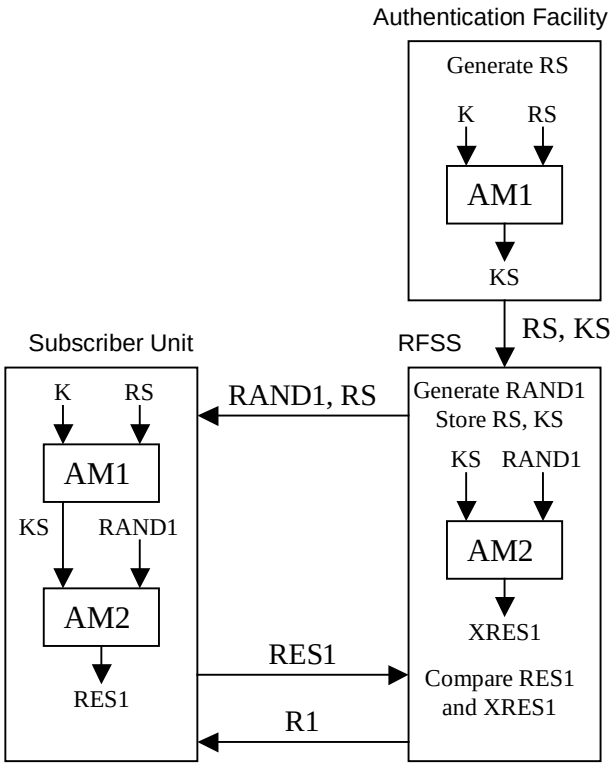


Figure 2.1-1 Challenge and Response Authentication Block Diagram

In this section, authentication of the SU is described as shown in Figure 2.1-1. An Authentication Facility (AF) uses Authentication Mechanism 1 (AM1) and K and the AF randomly generates a Random Seed, RS, to create the Session Authentication Key, KS, for the SU. The AF passes RS and KS to the Radio Frequency Sub-System (RFSS) in order to enable the RFSS to authenticate the SU.

The RFSS generates Random Challenge 1, RAND1, and uses KS with Authentication Mechanism 2 (AM2) to create the Expected Response 1, XRES1, to authenticate the SU. The RFSS passes RS to the SU so the SU can create KS using AM1. The RFSS passes RAND1 to the SU so the SU can create Response 1, RES1, using AM2. The SU passes RES1 to the RFSS so the RFSS can compare RES1 to XRES1. If RES1 and XRES1 match, the authentication is successful. Otherwise, the authentication is not successful. The result of the authentication is passed to the SU in the result (R1).

Several authentications may be done by the RFSS without having to contact the AF by using the same RS and KS and different RAND1.

2.2 Challenge and Response Mutual Authentication Block Diagram

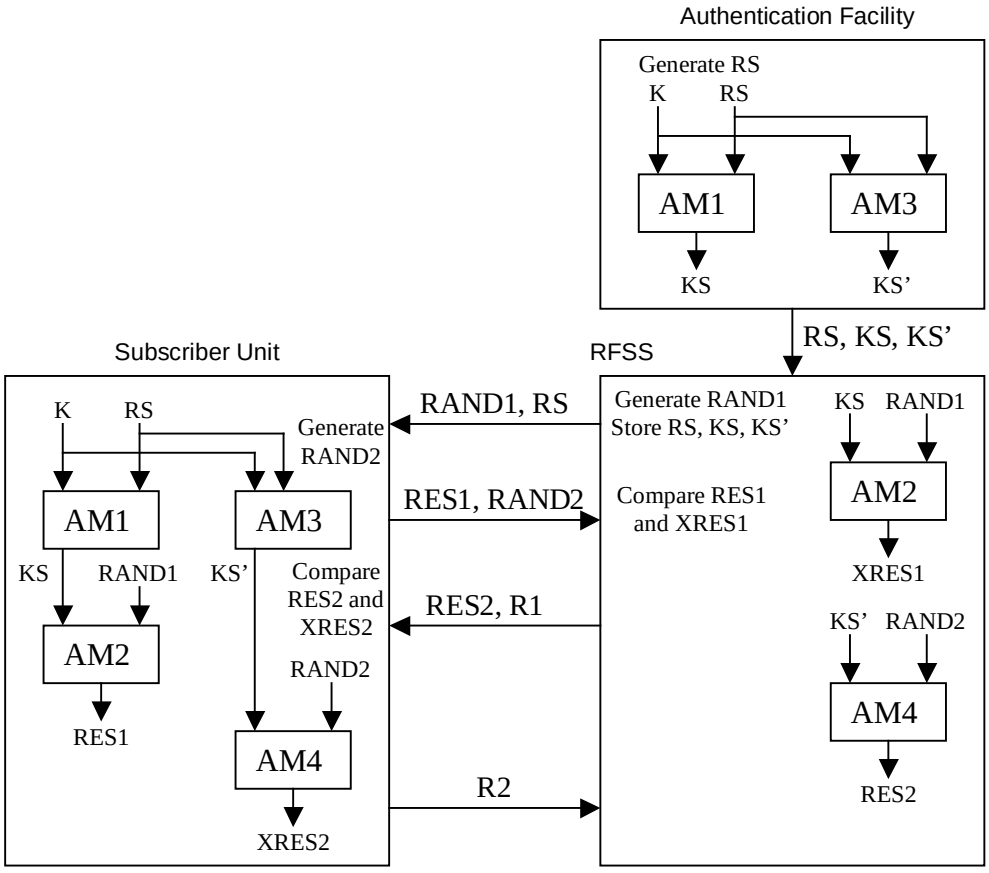


Figure 2.2-1 Challenge and Response Mutual Authentication Block Diagram

In this section, mutual authentication of SU and Radio Frequency Sub-System (RFSS) is described as shown in Figure 2.2-1. An Authentication Facility (AF) uses AM1 and K and randomly generates a Random Seed, RS, to create the Session Authentication Key, KS, for the SU. In addition, the AF uses Authentication Mechanism 3 (AM3) and K and randomly generates Random Seed, RS, to create the Mutual Session Authentication Key, KS', for the SU. The AF passes RS, KS and KS' to the RFSS, which enables the RFSS to authenticate the SU (using KS) and the SU to authenticate the RFSS (using KS').

The RFSS generates Random Challenge 1, RAND1, and uses KS with AM2 to create Expected Response 1, XRES1, to authenticate the SU. The RFSS passes RS to the SU so the SU can create KS using AM1. Since the SU wants to authenticate the RFSS, the SU will use RS to create KS' using AM3. The RFSS passes RAND1 to the SU so the SU can create Response 1, RES1, using AM2.

The SU passes RES1 to the RFSS so the RFSS can compare RES1 to XRES1. The SU will also generate and pass Random Challenge 2, RAND2, to the RFSS to authenticate the RFSS. A match of RES1 to XRES1 indicates a pass of authentication and Result 1, R1, will indicate authentication of the SU has passed. If RES1 and XRES1 do not match, then authentication has failed, R1 will indicate authentication of the SU has failed and Response 2, RES2, will not be sent to the SU.

When R1 indicates pass of authentication, the RFSS uses KS' and RAND2 with Authentication Mechanism 4 (AM4) to return RES2, to the SU so the SU can compare RES2 to Expected Response 2, XRES2. A match of RES2 to XRES2 indicates a pass of authentication of the RFSS and Result 2, R2, will indicate authentication of the RFSS has passed. If RES2 and XRES2 do not match, then authentication of the RFSS by the SU has failed and R2 will indicate authentication failure. R2 is sent from the SU to the RFSS.

Several authentications may be done by the RFSS without having to contact the AF by using the same RS and KS and different RAND1. Similarly, the SU may authenticate the RFSS several times with mutual authentication by using the same RS and KS' and different RAND2.

3 PROCEDURES AND OPERATIONAL DESCRIPTIONS

Authentication and mutual authentication is performed on the control channel. Authentication is initiated by the RFSS. If the SU wants to authenticate the RFSS the SU makes authentication mutual by challenging the RFSS during the authentication response. Example state diagrams are followed by some basic rules and Message Sequence Charts (MSCs).

3.1 Example State Diagrams

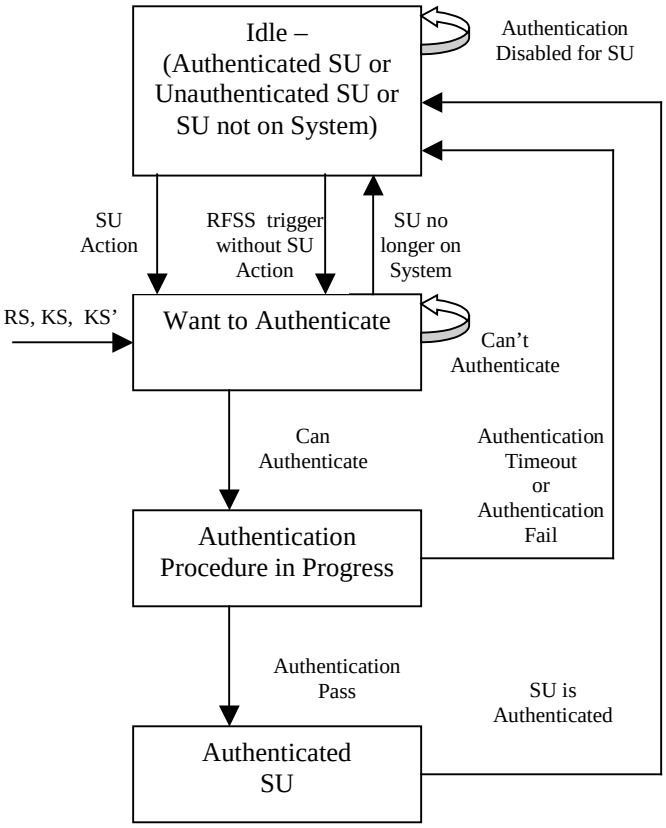


Figure 3.1-1 Example State Diagram for Authentication RFSS Focus

Figure 3.1-1 Example State Diagram for Authentication RFSS Focus applies to an authorized SU and is from the RFSS perspective. This description of the state diagram starts in the *Idle* state.

In the *Idle* state, the SU is not on the RFSS, has been authenticated or is not authenticated. If authentication is disabled for the SU, then the state will stay at Idle. When authentication is enabled for the SU, it is possible to transition out of the Idle state. To transition out of the *Idle* state, a SU action (such as unit registration) or a

RFSS trigger without SU action (such as verifying that the SU is still at a site) is needed. These transitions take the state to the *Want to Authenticate* state.

In the *Want to Authenticate* state, the RFSS has decided to authenticate the SU and will do so if possible. If the SU is held in the *Want to Authenticate* state, it may or may not be allowed to use the system depending on the security policies of the system and the reason that the system is unable to authenticate the SU. This example state diagram shows the case where the SU is allowed to use the system. In the *Want to Authenticate* state if the RFSS has RS, KS, KS' then authentication can be performed and a transition to *Authentication Procedure in Progress* state occurs. In the *Want to Authenticate* state if the RFSS does not have RS, KS, KS' then authentication cannot be performed and the state remains the same. If the SU is no longer on the system then the state transitions from the *Want to Authenticate* state to the *Idle* state.

In the *Authentication Procedure in Progress* state, the RFSS has initiated an authentication on the SU. The SU may optionally invoke mutual authentication to authenticate the FNE. If a service request (not involving authentication) is received from the SU, it may be ignored by the RFSS. In the *Authentication Procedure in Progress* state an Authentication Fail (including mutual) or Authentication Timeout takes the state back to Idle. When authentication fails, an existing authenticated SU on the system should not be effected by an adversary SU failing authentication. An Authentication Timeout can occur if the SU declines to respond to the authentication challenge from the RFSS or the SU declines to respond to the FNE response to a SU challenge during mutual authentication. Not responding should not benefit an adversary SU and the result of an adversary SU not responding should not interfere with a valid SU. The RFSS can also retry the challenge. When the authentication passes (including mutual if performed), the state transitions from the *Authentication Procedure in Progress* state to the *Authenticated SU* state.

In the *Authenticated SU* state, a SU is treated as authentic by the RFSS and the state transitions back to the *Idle* state. This is a valid SU.

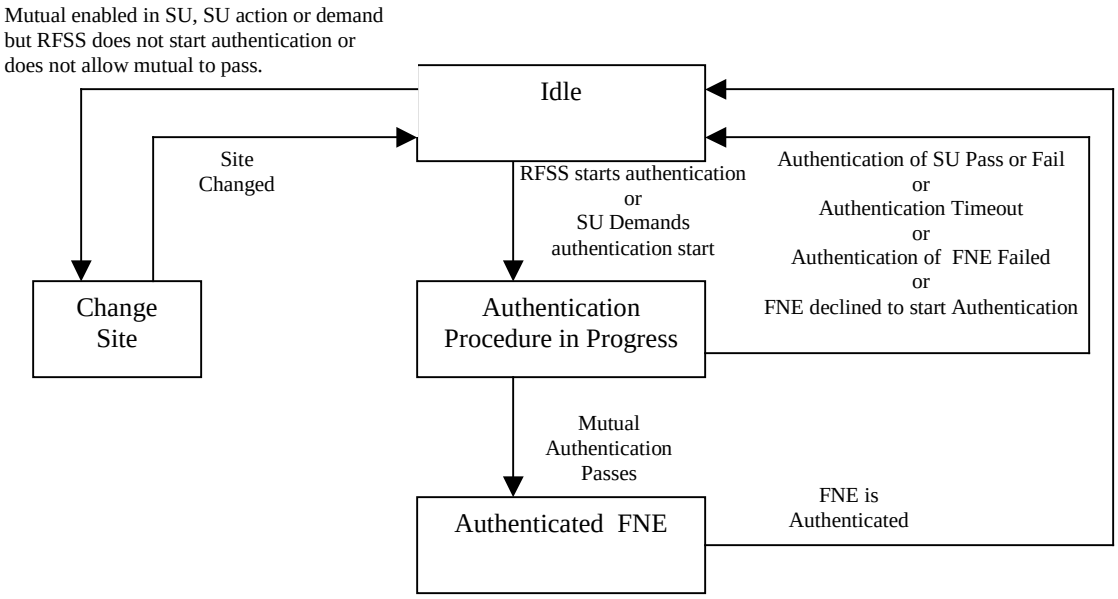


Figure 3.1-2 Example State Diagram for Authentication SU Focus

Figure 3.1-2 Example State Diagram for Authentication SU Focus applies to an authorized SU and is from the SU perspective. This description of the state diagram starts in the *Idle* state.

In the *Idle* state, the SU is not involved in any authentication transaction or was involved in an authentication transaction that did not allow mutual authentication to occur. The SU transitions to the *Authentication Procedure in Progress* state when the RFSS starts authentication by challenging the SU or by the SU demanding the RFSS start authentication. The RFSS may start authentication due to a SU action (such as unit registration) or a RFSS trigger without SU action (such as verifying that the SU is still at a site). An SU with mutual authentication enabled transitions state to the *Change Site* state when the FNE actively or passively declines to become authenticated on one or several attempts. The FNE declining mutual authentication should not benefit an adversary FNE in an attempt to trap the SU at that site.

In the *Change Site* state, the SU has decided to change sites in an attempt to avoid being trapped on an adversary FNE and to find a site that it can mutually authenticate with. The SU changes sites and tries to register on the new site. The state then goes to the Idle state with the expectation that the FNE will start authentication or the SU can demand authentication.

In the *Authentication Procedure in Progress* state, the RFSS has initiated an authentication on the SU. Authentication passing (non-mutual) or failing (non-mutual or mutual when SU fails) or Authentication Timeout or Authentication of FNE Failed or the FNE declines to start Authentication will change the state back to idle. An

Authentication Timeout can occur during mutual authentication if the FNE declines to respond to the challenge from the SU. When mutual authentication passes, the state transitions from the *Authentication Procedure in Progress* state to the *Authenticated FNE* state.

In the *Authenticated FNE* state, the FNE is treated as authentic by the SU and the state transitions back to the *Idle* state. This is a valid FNE.

3.2 Authentication Rules

This section describes some overall general rules followed by some specific message transaction based rules.

General Rules for Authentication:

1. Authentication shall be done on the control channel.

2. Authentication shall be initiated by the RFSS or a mutual authentication enabled SU demanding that the RFSS send a challenge.

3. If the authentication response RES1 is correct then the SU shall be considered valid by the RFSS.

4. If the authentication response RES1 is incorrect, then the SU may be ignored by the RFSS.

5. If there is no response from the SU then the action taken by the RFSS may be nothing or repeat the authentication command.

6. If the SU does not receive a result indicating authentication passed by the RFSS, then the SU may retry the message sequence if the authentication was initiated by the RFSS due to an SU action.

7. When authentication message sequence is started, an Authentication Timer will be started in the RFSS and SU. If the Authentication Timer expires (authentication message sequence did not complete), then the SU or RFSS with an expired Authentication Timer will revert to its state before the authentication sequence started. The RFSS and SU will use the same Authentication Timer value, the default value will be 30 seconds.

8. A SU commanded to authenticate, shall not send a separate service request until after the authentication response has been sent by the SU to the RFSS.

9. An adversary SU may fail authentication. Care should be taken so that this does not interfere with the status of a valid SU and the ability of a valid SU to acquire service on the system.

10. If the RFSS needs RS and KS to authenticate the SU, and it cannot obtain RS and KS, then the RFSS may allow an authorized SU access to the system or may not allow authorized SU access to the system depending on the security policy of the system. In the case where security policy allows access to the system, when the RFSS receives RS and KS, the RFSS should authenticate the SU. In the case where security policy does not allow access to the system, the SU will be denied with reason "the SU could not be authenticated at this time".

11. Authentication can be disabled for all SUs or for particular SU.

Message Transaction Based Rules for Authentication:

When the RFSS decides to authenticate the SU, the RFSS shall send a Authentication Demand OSP to the SU.

When the SU receives a Authentication Demand OSP, the SU shall respond with a Authentication Response ISP before sending any other ISP. If outside of registration the SU shall indicate it is a standalone authentication in the Authentication Response ISP.

When the RFSS receives the Authentication Response ISP from the SU and the SU passes authentication, the RFSS shall respond with:

a. If standalone, Acknowledge Response – FNE OSP
b. or if within unit registration, Unit Registration Response OSP
c. or if within location registration, Location Registration Response OSP

When the RFSS receives the Authentication Response ISP from the SU and the SU fails authentication, if not standalone and during Unit Registration the RFSS should respond with an extended form Unit Registration Response OSP with a Registration Value of REG_REFUSED, otherwise the RFSS should respond with Deny Response OSP with reason code "the SU has failed authentication". Sending a response enables the SU to do an orderly conclusion to the transaction.

3.3 Mutual Authentication Rules

This section describes some overall general rules for mutual authentication followed by some specific message transaction based rules for mutual authentication.

General Rules for Mutual Authentication:

1. If the authentication response RES2 from the RFSS is correct, then the RFSS shall be considered valid by the SU.

2. When the authentication response RES1 from the SU fails, the RFSS shall not send a response RES2 to the SU challenge RAND2.

3. When the authentication response RES2 from the RFSS fails, the SU may abandon the site and attempt to use another site.

4. When the RFSS does not respond to the challenge RAND2 from the SU, the SU may retry the challenge RAND2 or may abandon the site and attempt to use another site.

5. When the SU expects a response to R2 and the RFSS does not respond, SU may retry the response R2 or may abandon the site and attempt to use another site.

6. The FNE shall be capable of mutual authentication.

7. When the SU is configured for mutual authentication, the SU shall invoke mutual authentication.

Message Transaction Based Rules for Mutual Authentication:

When the SU decides to authenticate the RFSS during authentication of the SU, the SU shall respond to an Authentication Demand OSP with an Authentication Response Mutual ISP. If outside of registration the SU shall indicate it is a standalone authentication in the Authentication Response Mutual ISP.

When the SU receives the Authentication FNE Response OSP from the RFSS and the RFSS passes authentication, the SU shall respond with Authentication FNE Result ISP with R2 indicating FNE passed authentication. If outside of registration the SU shall indicate it is a standalone authentication in the Authentication FNE Result ISP.

When the RFSS receives the Authentication FNE Result ISP from the SU indicating that the FNE passed authentication, the RFSS shall respond with:

a. If standalone, Acknowledge Response – FNE OSP
b. or if within unit registration, Unit Registration Response OSP
c. or if within location registration, Location Registration Response OSP

When the RFSS receives the Authentication Response Mutual ISP from the SU and the SU fails authentication, if not standalone and during Unit Registration the RFSS should respond with an extended form Unit Registration Response OSP with a Registration Value of REG_REFUSED, otherwise the RFSS should respond with

Deny Response OSP with reason code “the SU has failed authentication”. Sending a response enables the SU to do an orderly conclusion to the transaction.

When the SU receives the Authentication FNE Response OSP from the RFSS and the RFSS fails authentication, the SU shall respond with Authentication FNE Result ISP with R2 indicating FNE failed authentication. If outside of registration the SU shall indicate it is a standalone authentication in the Authentication FNE Result ISP.

When the RFSS receives the Authentication FNE Result ISP from the SU indicating that the FNE failed authentication, if not standalone and during Unit Registration the RFSS should respond with an extended form Unit Registration Response OSP with a Registration Value of REG_REFUSED, otherwise the RFSS should respond with Deny Response OSP with reason code “the FNE has failed authentication”. Sending a response enables the SU to do an orderly conclusion to the transaction.

When the RFSS declines to send an Authentication Demand OSP to challenge the SU, after the message sequence the SU may send an Authentication SU Demand ISP to request that the RFSS start an authentication. The SU should not send an Authentication SU Demand ISP during a registration message sequence.

3.4 Standalone Authentication Message Sequence Charts (MSC)

This section shows several representative MSCs that may be used by the system.

3.4.1 MSC for Challenge and Response Authentication Passes

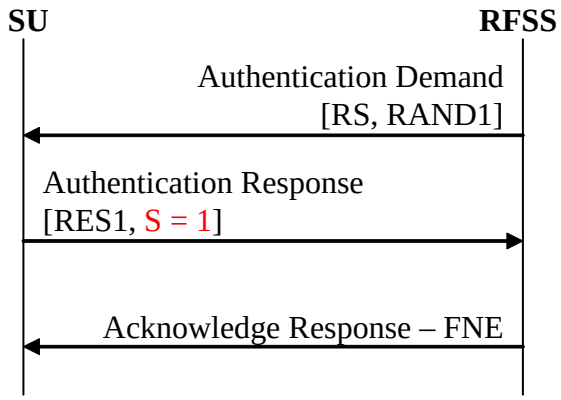


Figure 3.4-1 MSC for Challenge and Response Authentication Passes

In Figure 3.4-1, the RFSS decides to authenticate the SU by sending an Authentication Demand OSP. The SU responds with an Authentication Response ISP indicating standalone S=%1. When authentication passes (RES1 equals XRES1), the RFSS sends an Acknowledge Response – FNE OSP to the SU. When authentication fails is shown in Figure 3.4-2.

3.4.2 MSC for Challenge and Response Authentication Fails

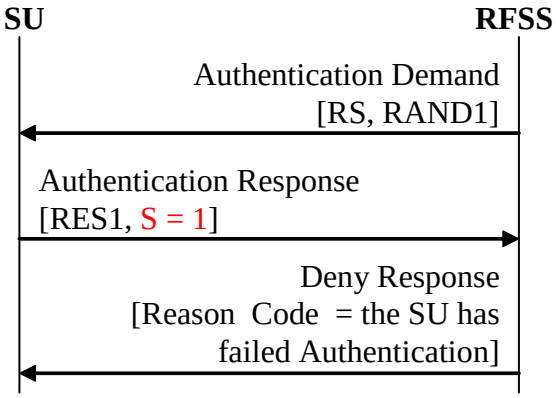


Figure 3.4-2 MSC for Challenge and Response Authentication Fails

In Figure 3.4-2, the RFSS decides to authenticate the SU by sending an Authentication Demand OSP. The SU responds with an Authentication Response ISP indicating standalone S=%1. In this case, authentication of the SU fails (RES1 not equal XRES1) and the SU is probably an adversary. The RFSS responds with a Deny Response OSP with a Deny Response Reason Code of “the SU has failed authentication”.

3.4.3 MSC Mutual Challenge and Response Authentication Passes

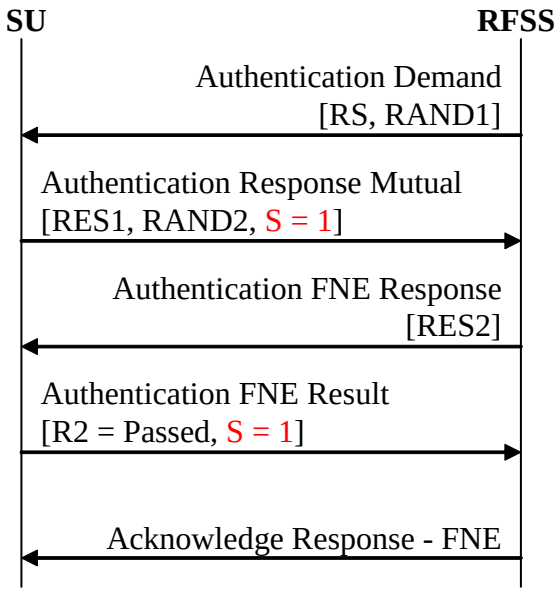


Figure 3.4-3 MSC Mutual Challenge and Response Authentication Passes

In Figure 3.4-3, the RFSS decides to authenticate the SU by sending an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating standalone S=%1. When authentication of the SU passes, the RFSS sends the Authentication FNE Response OSP to the SU. The SU sends the Authentication FNE Result ISP indicating standalone S=%1 to the RFSS. In this case, authentication of the RFSS passes (RES2 equals XRES2), R2 in Authentication FNE Result ISP will be passed. The RFSS responds with an Acknowledge Response – FNE. When authentication of the RFSS fails (RES2 not equal XRES2) will deny the SU as shown in Figure 3.4-5.

When authentication of the SU fails (RES1 not equal XRES1), the RFSS will not provide an authentication FNE response as shown in Figure 3.4-4.

3.4.4 MSC Mutual Challenge and Response Authentication of SU Fails

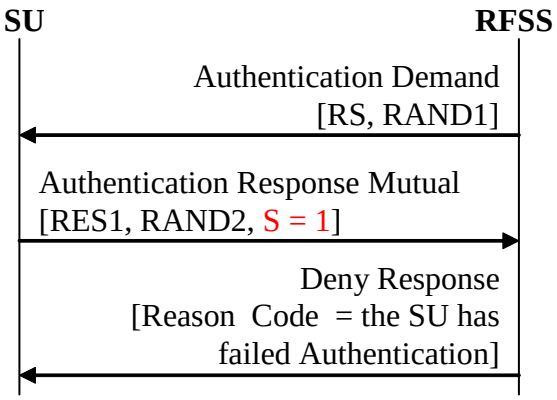


Figure 3.4-4 Mutual Challenge and Response Authentication of SU Fails

In Figure 3.4-4, the RFSS decides to authenticate the SU by sending an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating standalone S=%1. In this case, authentication of the SU fails (RES1 not equal XRES1) and the SU is probably an adversary. The RFSS responds with a Deny Response OSP with a Deny Response Reason Code of "the SU has failed authentication".

3.4.5 MSC Mutual Challenge and Response Authentication of RFSS Fails

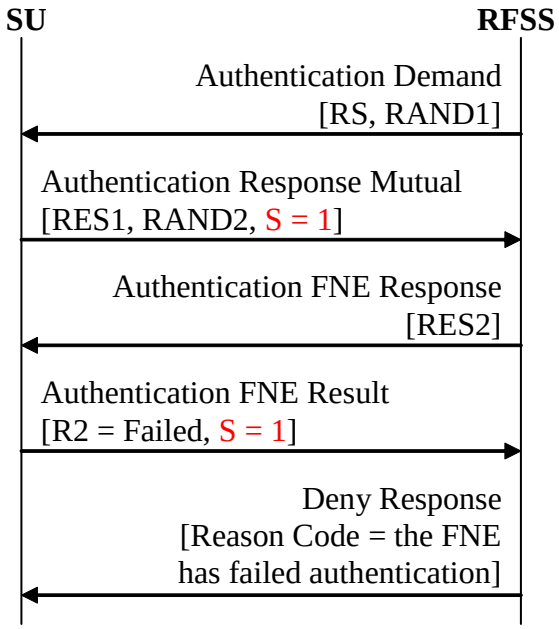


Figure 3.4-5 MSC Mutual Challenge and Response Authentication RFSS Fails

In Figure 3.4-5, the RFSS decides to authenticate the SU by sending an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating standalone S=%1. The RFSS sends the Authentication FNE Response OSP to the SU. An adversary RFSS most likely would represent the SU as passing authentication. The SU sends the Authentication FNE Result ISP to the RFSS indicating standalone S=%1. In this case, authentication of the SU passes (RES1 equals XRES1), but authentication of the RFSS has failed (RES2 not equal XRES2) and R2 in Authentication FNE Result ISP will be failed. The RFSS responds with a Deny Response OSP with a Deny Response Reason Code of "the FNE has failed authentication".

3.5 Registration Message Sequences Charts (MSC)

The following MSCs show authentication and mutual authentication at unit registration. Authentication and mutual authentication at location registration may also be done. The SU starts the sequences, but never initiates authentication. The RFSS may initiate authentication in response to registration.

3.5.1 MSC Unit Challenge and Response Authentication Passes

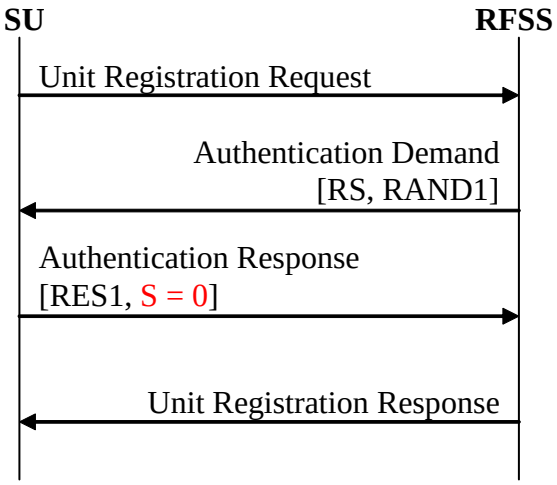


Figure 3.5-1 MSC Challenge and Response Authentication Passes During Unit Registration

In Figure 3.5-1, the SU requests access to the system by sending a Unit Registration Request ISP. The RFSS does not know if the SU is valid, so the RFSS responds with an Authentication Demand OSP. The SU responds with an Authentication Response OSP indicating not standalone S=%0. In this case, authentication of the SU passes (RES1 equals XRES1) so the RFSS sends a Unit Registration Response OSP to the valid SU. When authentication fails is shown in Figure 3.5-2.

3.5.2 MSC Unit Challenge and Response Authentication Fails

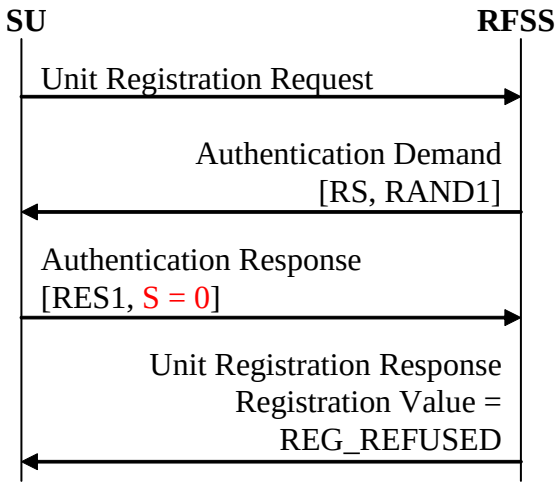


Figure 3.5-2 MSC Challenge and Response Authentication Fails During Unit Registration

In Figure 3.5-2, the SU requests access to the system by sending a Unit Registration Request ISP. The RFSS does not know if the SU is valid, so the RFSS responds with an Authentication Demand OSP. The SU responds with an Authentication Response OSP indicating not standalone S=%0. In this case, authentication of the SU fails (RES1 not equal XRES1) and the SU is probably an adversary. The RFSS responds with an extended form Unit Registration Response OSP with a Registration Value of REG_REFUSED.

3.5.3 MSC Mutual Challenge and Response Authentication Passes

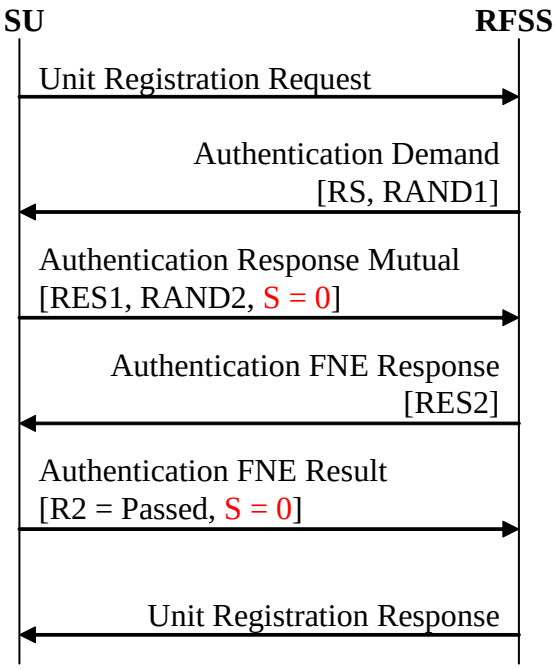


Figure 3.5-3 MSC Mutual Challenge and Response Authentication During Unit Registration

In Figure 3.5-3, the SU requests access to the system by sending a Unit Registration Request ISP. The RFSS does not know if the SU is valid, so the RFSS responds with an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating not standalone S=%0. The RFSS sends the Authentication FNE Response OSP to the SU. The SU sends the Authentication FNE Result ISP to the RFSS indicating not standalone S=%0. In this case, authentication of the SU passes (RES1 equals XRES1) and authentication of the RFSS passes (RES2 equals XRES2) so the RFSS sends a Unit Registration Response OSP.

When authentication of the SU fails (RES1 not equal XRES1), the RFSS will not send an Authentication FNE Response OSP. This is shown in Figure 3.5-4.

3.5.4 MSC Mutual Challenge and Response Authentication Fails

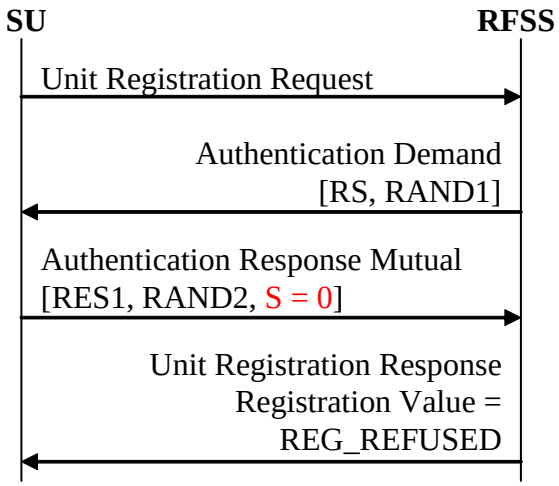


Figure 3.5-4 MSC Mutual Challenge and Response Authentication During Unit Registration SU Fails

In Figure 3.5-4, the SU requests access to the system by sending a Unit Registration Request ISP. The RFSS does not know if the SU is valid, so the RFSS responds with an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating not standalone S=%0. However, the authentication of the SU fails (RES1 not equal XRES1) and the SU is probably an adversary. The RFSS responds with an extended form Unit Registration Response OSP with a Registration Value of REG_REFUSED.

3.5.5 MSC Mutual Challenge and Response Authentication RFSS Fails

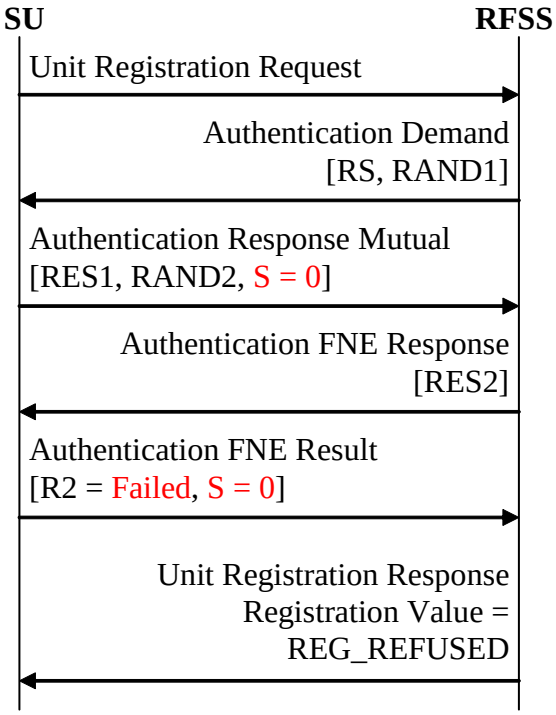


Figure 3.5-5 MSC Mutual Challenge and Response Authentication During Unit Registration RFSS Fails

3.5.6 In Figure 3.5-5, the SU requests access to the system by sending a Unit Registration Request ISP. The RFSS does not know if the SU is valid, so the RFSS responds with an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating not standalone S=%0. The RFSS sends the Authentication FNE Response OSP to the SU. An adversary RFSS most likely would represent the SU as passing authentication. The SU sends the Authentication FNE Result ISP to the RFSS indicating not standalone S=%0. In this case, authentication of the SU passes (RES1 equals XRES1), but authentication of the RFSS has failed (RES2 not equal XRES2) and R2 in Authentication FNE Result ISP will be failed. The RFSS responds with an extended form Unit Registration Response OSP with a Registration Value of REG_REFUSED.

MSC SU Authentication Demand

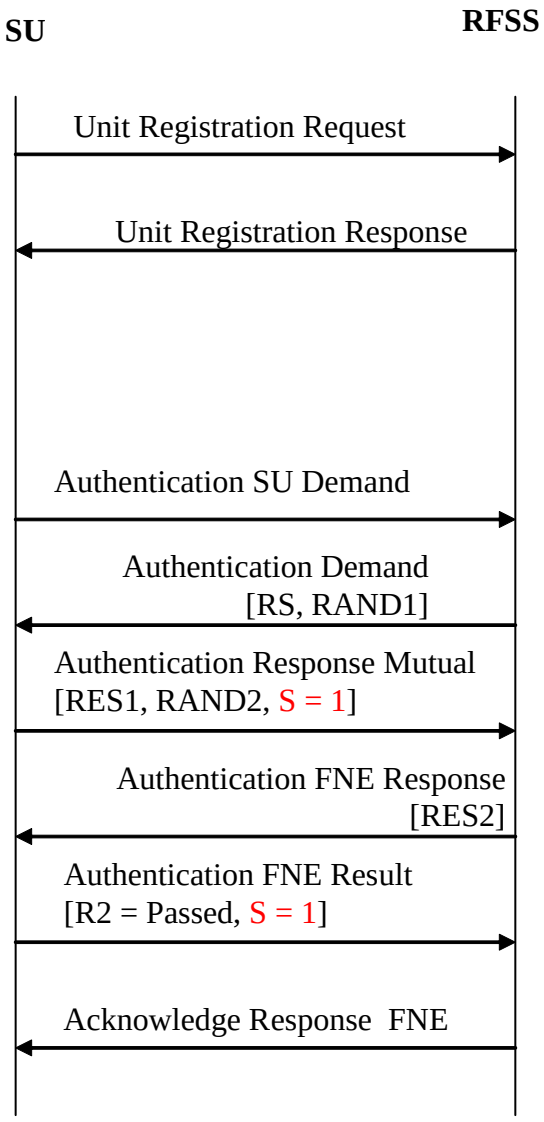


Figure 3.5-6 MSC Authentication SU Demand

In Figure 3.5-6, the SU requests access to the system by sending a Unit Registration Request ISP. The RFSS declines to authenticate the SU and responds with a Unit Registration Response OSP. The SU which wants to be authenticated sends an Authentication SU Demand ISP to request authentication be started. The RFSS responds with an Authentication Demand OSP. The SU responds with an Authentication Response Mutual ISP to authenticate the RFSS, indicating standalone S=%1. The RFSS sends the Authentication FNE Response OSP to the SU. The SU sends the Authentication FNE Result ISP indicating standalone S=%1 to the RFSS. In this case, authentication of the SU passes (RES1 equals XRES1)

and authentication of the RFSS passes (RES2 equals XRES2) so the RFSS sends an Acknowledge Response FNE OSP.

Upon receiving the Authentication SU Demand ISP, if the RFSS is not capable of authenticating the SU, the RFSS sends a Deny Response OSP with a Deny Response Reason Code of “the SU could not be authenticated at this time”.

4 CONTROL CHANNEL MESSAGES

The control channel messages to support challenge and response authentication and challenge and response mutual authentication are in reference [1] and are listed below.

- Authentication Demand OSP
- Authentication Response ISP
- Authentication Response Mutual ISP
- Authentication FNE Response OSP
- Authentication FNE Result ISP
- Authentication SU Demand ISP

5 KEY MANAGEMENT AND PROVISIONING

This section describes key management guidelines and how the system is provisioned with K.

5.1 Key Management

The authentication key (K) (one per SUID) is intended to be given to the SU once as described in Section 5.2 Provisioning. Therefore, measures should be taken to reduce the exposure of K to compromise. These measures include confidential protection of K while it is stored in the AF and provisioning system along with limited access to and transfer of K with the system. The transfer of K is limited by sending RS, KS and KS' into the RFSS instead of K as shown in Figure 2.1-1 Challenge and Response Authentication Block Diagram and Figure 2.2-1 Challenge and Response Mutual Authentication Block Diagram .

The KS is used to do the authentication to avoid exposure of K. Extensive repeated use of the same KS could help an adversary. To avoid this, a crypto period can be applied to KS by having the AF periodically change RS to change KS (see Figure 2.1-1 AM1). For mutual authentication, the same logic applies to KS' (see Figure 2.2-1 AM3).

Key Management Provisioning (Informative)

In a system that supports OTAR (reference [6]), a K per SUID may also be sent to the SU over-the-air for initial provisioning and to change K afterwards. Systems that do not have OTAR shall not have the capability to send K over-the-air to the SU.

5.2 Provisioning (Informative)

The authentication key (K) must be provisioned in the SU and AF for authentication to be possible.

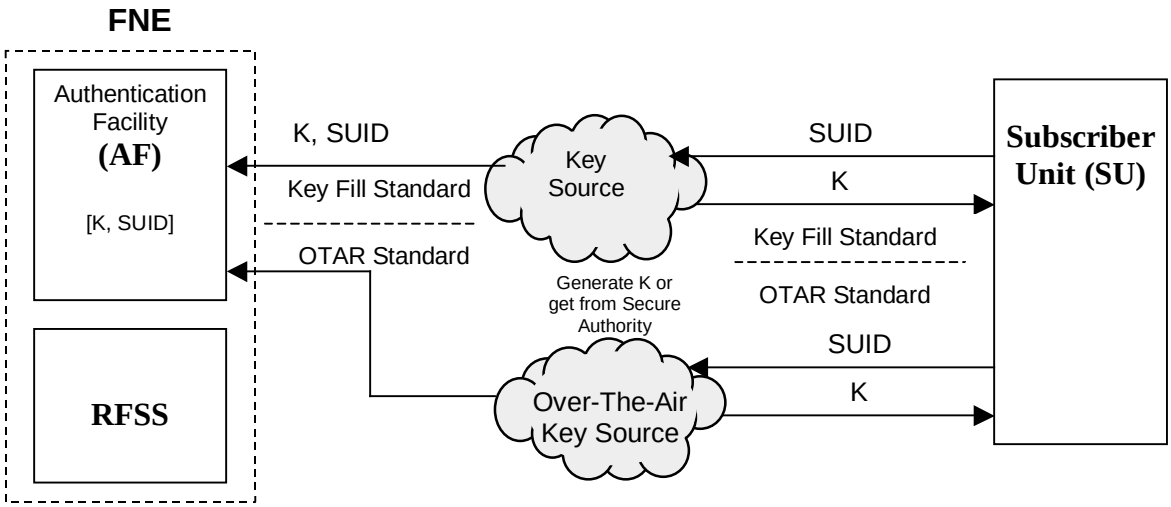


Figure 5.2-1 Example Provisioning Information Flow

In Figure 5.2-1, an example of information flows to provision the system for authentication are shown. The Key Source or Over-The-Air Key Source may generate K or get it from a Secure Authority. The Key Source receives the SUID from the SU and gives K to the SU. The Key Source gives the K-SUID pair to the AF. The Over-The-Air Key Source receives the SUID from the SU over-the-air and gives K to the SU over-the-air. The Over-The-Air Key Source gives the K-SUID pair to the AF.

Once the K-SUID pair exists in the AF, the AF may send RS, KS and KS' to the RFSS as shown in Figure 2.1-1 or Figure 2.2-1.

The programming of K into the SU and transfer of K-SUID to the FNE is described in the Key Fill Device Interface Protocol document[1] (reference [5]). The Over-The-Air programming of K into the SU and subsequent transfer of K-SUID to the FNE is described in the Over-The-Air-Rekeying (OTAR) Protocol document[1] (reference [6]). The programming of the SUID into the SU and FNE is manufacturer specific and is beyond the scope of this document.

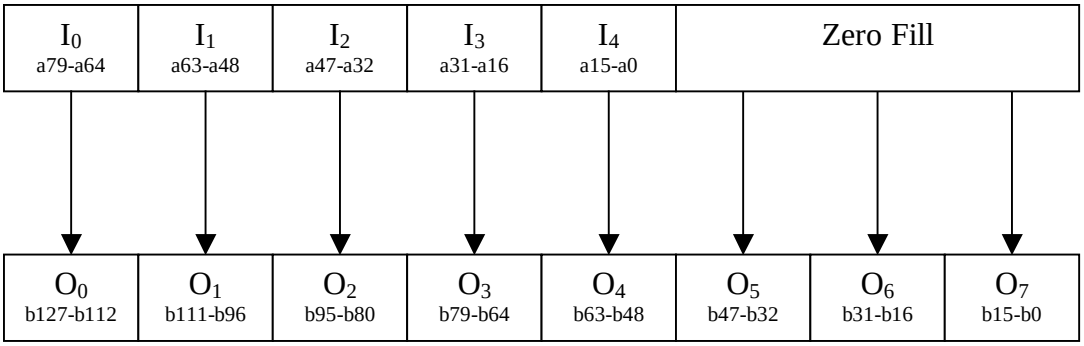
[1] This document currently does not contain information on authentication. It is intended that the document will be updated for authentication.

6 AUTHENTICATION MECHANISM (AM) AND AES CRYPTO DETAILS

The base algorithm used for authentication shall be AES using a 128 bit key size (called AES-128 in reference [2]) operating in Electronic Codebook (ECB) mode (reference [3]). Some authentication parameters need to be expanded to match the AES-128 128 bit block size or need to be reduced from the 128 block size to match the air interface limitations. Each authentication mechanism below is a different instance of AES-128 operating in ECB mode.

6.1 AM1 (K, RS, KS)

AM1 shall input K and RS, and output KS. Knowledge of RS and KS should not reveal K. An expansion is needed on RS (80 bits) to match the AES-128 block size (128 bits). The expansion is shown in Figure 6.1-1 and the block diagram of AM1 is shown in Figure 6.1-2.



$O_0 = I_0$ $O_4 = I_4$
$O_1 = I_1$ $O_5 = 0x0000$
$O_2 = I_2$ $O_6 = 0x0000$
$O_3 = I_3$ $O_7 = 0x0000$

Figure 6.1-1 Expansion of RS from 80 bits to 128 bits

The expansion of RS from 80 bits to 128 bits shown in Figure 6.1-1 is needed to match the AES-128 block size of 128 bits. The most significant input bit is a79 and the least significant input bit is a0. The 16 bit input words range from most significant input word I_0 to least significant input word I_4. The most significant output bit is b127 and the least significant input bit is b0. The 16-bit output words range from most significant output word O_0 to least significant output word O_7. Words I_0 thru I_4 are directly put into O_0 thru O_4. The remaining O_5 thru O_7 are zero filled as shown in Figure 6.1-1.

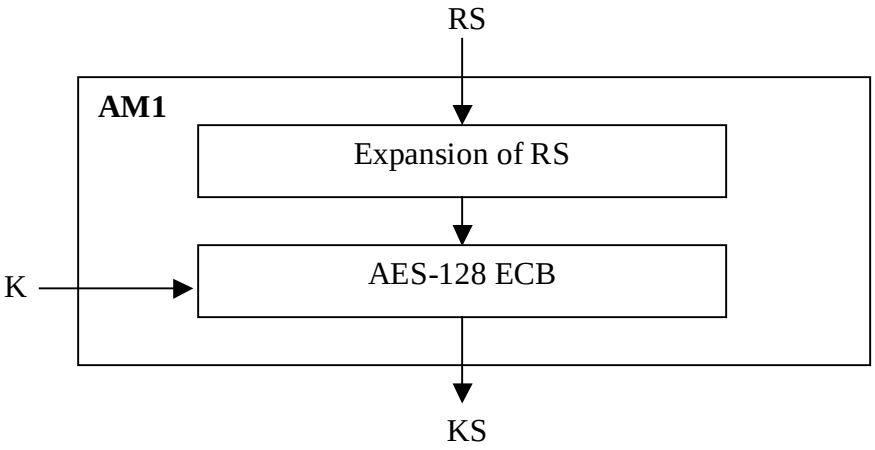


Figure 6.1-2 AM1 Block Diagram

The details of AM1 are shown in Figure 6.1-2. AM1 shall input K (128 bits) and RS (80 bits), and output KS (128 bits). RS is expanded from 80 bits to 128 bits as shown in Figure 6.1-1 and is plain text in for AES-128 operating in ECB mode with the encryption key being K. Cipher text out from the AES-128 operation is KS.

6.2 AM2 (KS, RAND1, RES1)

AM2 shall input KS and RAND1, and output RES1 or its equivalent XRES1. Knowledge of RAND1 and RES1 should not reveal KS. An expansion is needed on RAND1 (40 bits) to match the AES-128 block size (128 bits). The expansion is shown in Figure 6.2-1. A reduction is needed for RES1 (32 bits) from the 128-bit AES-128 output block size. This reduction is shown in Figure 6.2-2. The block diagram for AM2 is shown in Figure 6.2-3.

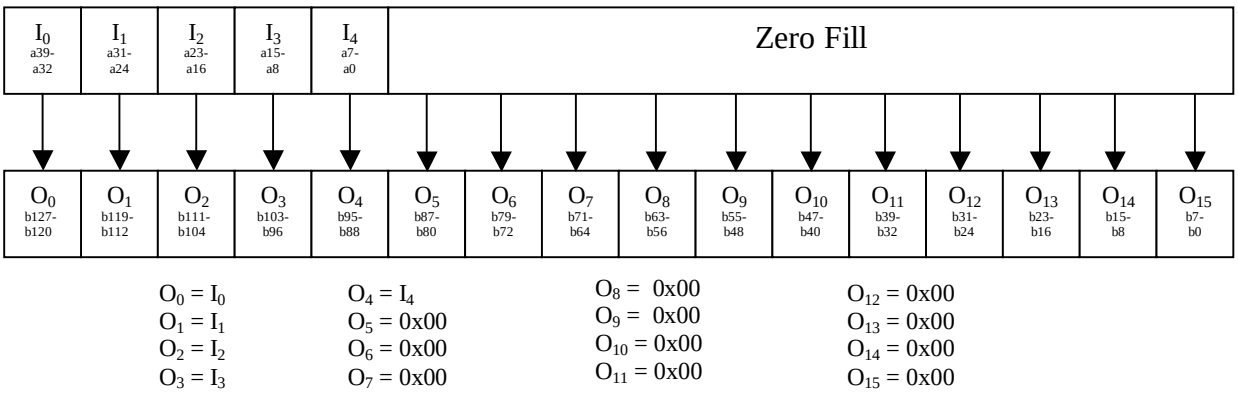


Figure 6.2-1 Expansion of RAND from 40 bits to 128 bits

The expansion of RAND from 40 bits to 128 bits shown in Figure 6.2-1 is needed to match the AES-128 block size of 128 bits. The most significant input bit is a39 and the least significant input bit is a0. The input octets range from most significant input octet, I_0, to least significant input octet, I_4. The most significant output bit is b127 and the least significant input bit is b0. The output octets range from most significant output octet, O_0, to least significant output octet, O_{15}. Octets I_0 thru I_4 are directly put into O_0 thru O_4. The remaining O_5 thru O_{15} are zero filled as shown in Figure 6.2-1.

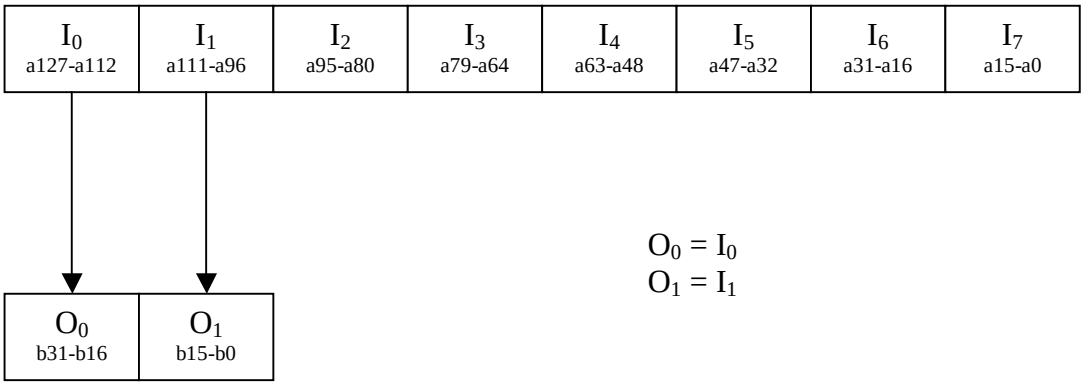


Figure 6.2-2 Reduction of RES from 128 bits to 32 bits

The reduction of RES from AES-128 block size of 128 bits to 32 bits due to air interface limitations is shown in Figure 6.2-2. The most significant input bit is a127 and the least significant input bit is a0. The 16-bit input words range from most significant input word I_0 to least significant input word I_7. The most significant output bit is b31 and the least significant input bit is b0. The 16-bit output words range from most significant output word O_0 to least significant output word O_1. Input words I_0 I_1 are used as outputs words O_0 O_1.

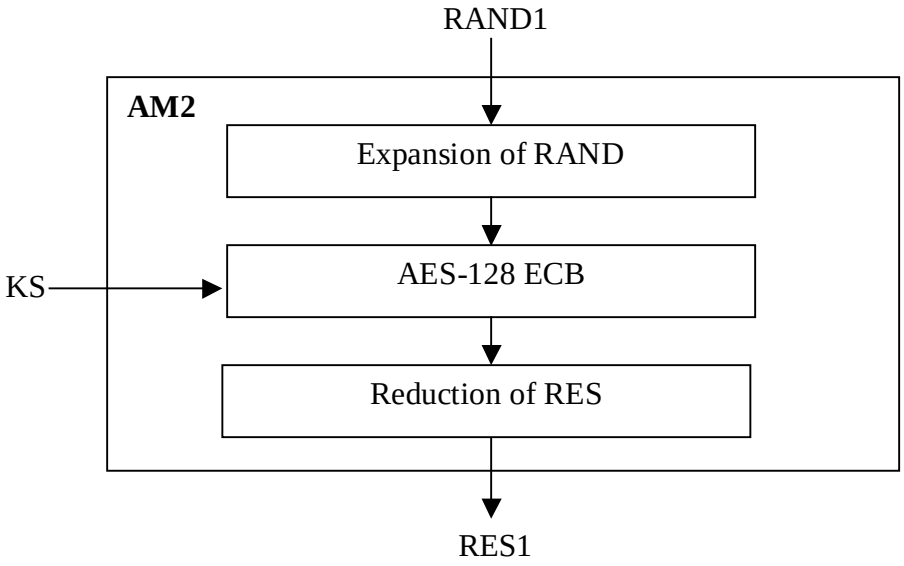


Figure 6.2-3 AM2 Block Diagram

The details of AM2 are shown in Figure 6.2-3. AM2 shall input KS (128 bits) and RAND1 (40 bits), and output RES1 (32 bits). RAND1 is expanded from 40 bits to 128 bits as shown in Figure 6.2-1 and is plain text in for AES-128 operating in ECB mode with the encryption key being KS. Cipher text out from the operation is 128 bits RES. The 128 bit RES is input to the reduction of RES operation as shown in Figure 6.2-2 which outputs a 32 bit RES to become the output RES1 of AM2. When AM2 is used to create an expected response (XRES1) the output RES1 is used as XRES1.

6.3 AM3 (K, RS, KS')

AM3 shall input K and RS, and output KS'. Knowledge of RS and KS' should not reveal K. An expansion is needed on RS (80 bits) to match the AES-128 block size (128 bits). This expansion is shown in Figure 6.1-1. The block diagram for AM3 is shown in Figure 6.3.

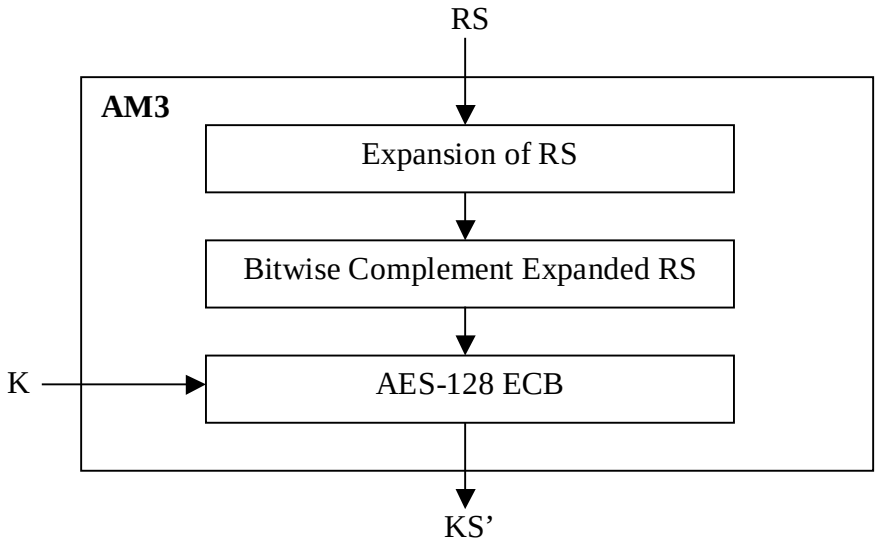


Figure 6.3-1 AM3 Block Diagram

The details of AM3 are shown in Figure 6.3-1. AM3 shall input K (128 bits) and RS (80 bits), and output KS' (128 bits). RS is expanded from 80 bits to 128 bits as shown in Figure 6.1-1 followed by a bitwise complement of the expanded RS and then is plain text in for AES-128 operating in ECB mode with the encryption key being K. Cipher text out from the AES-128 operation is KS'.

6.4 AM4 (KS', RAND2, RES2)

AM4 shall input KS' and RAND2, and output RES2 or its equivalent XRES2. Knowledge of RAND2 and RES2 should not reveal KS'. An expansion is needed on RAND2 (40 bits) to match the AES-128 block size (128 bits). The expansion is shown in Figure 6.2-1. A reduction is need for RES2 (32 bits) from the 128-bit AES-128 output block size. This reduction is shown in Figure 6.2-2. The block diagram for AM4 is shown in Figure 6.4-1.

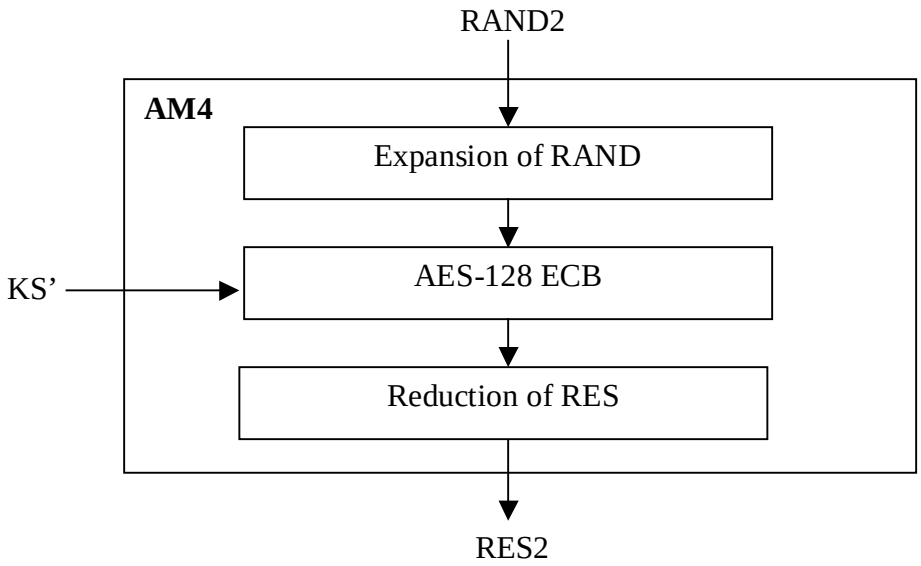


Figure 6.4-1 AM4 Block Diagram

The details of AM4 are shown in Figure 6.4-1. AM4 shall input KS' (128 bits) and RAND2 (40 bits), and output RES2 (32 bits). RAND2 is expanded from 40 bits to 128 bits as shown in Figure 6.2-1 and is plain text in for AES-128 operating in ECB mode with the encryption key being KS'. Cipher text out from the operation is 128 bits RES. The 128 bit RES is input to the reduction of RES operation as shown in Figure 6.2-2 which outputs a 32 bit RES to become the output RES2 of AM4. When AM4 is used to create an expected response (XRES2) the output RES2 is used as XRES2.

6.5 Parameters and Sizes

This section contains Table 6.5-1 Parameter Sizes, which shows authentication parameters and their size in bits.

Parameter	Size in Bits
K	128
KS	128
KS'	128
RAND1	40
RAND2	40
RES1	32
RES2	32
RS	80
XRES1	32
XRES2	32

Table 6.5-1 Parameter Sizes

6.6 Example Data

This section contains example data for the algorithms.

Authentication Mechanism 1 (AM1) sample data:

```
K              = 0001 0203 0405 0607 0809 0a0b 0c0d 0e0f
RS             = 38ae c829 33b1 7f80 249d
Expanded RS    = 38ae c829 33b1 7f80 249d 0000 0000 0000
KS             = 0524 30bd af39 e82f d0dd d698 c02f b036
```

Authentication Mechanism 2 (AM2) sample data:

```
KS             = 0524 30bd af39 e82f d0dd d698 c02f b036
RAND1          = 4d 92 5a f6 08
Expanded RAND1 = 4d 92 5a f6 08 00 00 00 00 00 00 00 00 00 00
AES Output     = 3e00 faa8 f0c7 e864 0e92 7bb3 41b5 d44a
RES1           = 3e00 faa8
```

Authentication Mechanism 3 (AM3) sample data:

```
K              = 0001 0203 0405 0607 0809 0a0b 0c0d 0e0f
RS             = 38ae c829 33b1 7f80 249d
Expanded RS    = 38ae c829 33b1 7f80 249d 0000 0000 0000
Complement RS  = c751 37d6 cc4e 807f db62 ffff ffff ffff
KS'            = 69d5 dc08 023c 4652 cc71 d5cd 1e74 e104
```

Authentication Mechanism 4 (AM4) sample data:

```
KS'            = 69d5 dc08 023c 4652 cc71 d5cd 1e74 e104
RAND2          = 6e 78 4f 75 bd
Expanded RAND2 = 6e 78 4f 75 bd 00 00 00 00 00 00 00 00 00 00
AES Output     = b3ad 16e1 7ad4 49c3 5459 f041 21a4 2989
RES2           = b3ad 16e1
```

THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TIA represents the global information and communications technology (ICT) industry through standards development, advocacy, tradeshows, business opportunities, market intelligence and world-wide environmental regulatory analysis. With roots dating back to 1924, TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications.

TIA members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment. TIA co-owns the SUPERCOMM® tradeshow and is accredited by the American National Standards Institute (ANSI).

ADVANCING GLOBAL COMMUNICATIONS

HEADQUARTERS
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834
+1.703.907.7700
+1.703.907.7727 (fax)

tiaonline.org