

1  
3GPP2 A.S0006-0 v1.0

Date: December 2004



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

---

2  
3  
4  
**Interoperability Specification (IOS) for Hybrid Mobile  
Station / Access Terminal (HAT) Authentication, Using  
the CAVE Algorithm**

5  
6  
7  
8  
**3GPP2 Publication Version**

*COPYRIGHT* © 2004, 3GPP2

*3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.*



## Table of Contents

1	<b>Table of Contents</b>		
2	Foreword.....		iii
3	1 Introduction.....		1-1
4	1.1 Scope.....		1-1
5	1.2 Document Convention .....		1-1
6	1.3 Normative References.....		1-2
7	1.3.1 3GPP2 .....		1-2
8	1.3.2 TIA/EIA .....		1-2
9	1.3.3 Other .....		1-2
10	1.4 Terminology.....		1-3
11	1.4.1 Acronyms.....		1-3
12	1.4.2 Definitions .....		1-3
13	1.5 Reference Model.....		1-4
14	1.6 Assumptions.....		1-4
15	2 HAT HRPD Network Access Authentication Using the CAVE Algorithm.....		2-1
16	2.1 HAT Requirements .....		2-1
17	2.2 AN/PCF Requirements .....		2-1
18	2.3 Home AN-AAA Requirements.....		2-1
19	Annex A Message Exchange Example.....		A-1
20			
21			

## Table of Figures

1  
2  
3  
4  
5  
6  
7

Figure 1.5-1	Reference Architecture for HAT Authentication.....	1-4
Figure Annex A-1	HAT Authentication Message Flow .....	A-1

## 1 **Foreword**

---

2 (This foreword is not part of this specification.)

3 This document was produced by Working Groups TR45.4 of the Telecommunications Industry Associat-  
4 ion and TSG-A of the Third Generation Partnership Project 2. This document was developed in accord-  
5 ance with TIA/EIA and 3GPP2 procedural guidelines, and represents the consensus position of the  
6 Working Groups.

7 Suggestions for improvement of this specification are welcome. They should be sent to:

8 Telecommunications Industry Association  
9 Engineering Department  
10 Suite 300  
11 250 Wilson Boulevard  
12 Arlington, VA 22201 USA

13  
14

1

This page intentionally left blank.

2

# 1 Introduction

---

## 1.1 Scope

---

High Rate Packet Data (HRPD) network access authentication is described in [1] and [2]. This document provides alternative procedures that allow a properly configured Hybrid mobile station / Access Terminal (HAT) to use its cdma2000<sup>®1</sup> 1x access network authentication credentials and the Cellular Authentication and Voice Encryption (CAVE) algorithm (refer to [6]) when accessing an HRPD network that requires HRPD network access authentication.

Because HRPD network access authentication is optional, it may not be invoked by every HRPD network. If it is invoked by an HRPD network, the network initiates the Challenge Handshake Authentication Protocol (CHAP) [8]. In an HRPD network that complies with [2], CHAP is used between the Access Network (AN) and the HAT. In an HRPD network that complies with [1], CHAP is used between the Packet Control Function (PCF) and the HAT. CHAP specifies that the AN/PCF sends a CHAP Challenge message to the HAT, and the HAT returns a CHAP Response message to the AN/PCF. After receiving the CHAP Response message, the AN/PCF sends both its challenge and the HAT's response to its Access Network-Authentication, Authorization, and Accounting (AN-AAA) function. The home AN-AAA authenticates the HAT and returns the results to the AN/PCF.

For this feature of authenticating the HAT by using its cdma2000 1x access network authentication credentials and the CAVE algorithm, the HAT treats the challenge in the CHAP Challenge message as a global random challenge (refer to [3], [4] and [5]). When the CHAP challenge message is received, the HAT uses the challenge as input to the Run CAVE function on its Removable User Identity Module (R-UIM) (refer to [3], [4] and [5]) and places the result in the CHAP response message.

When the home AN-AAA receives the HRPD network access authentication request from the AN/PCF (refer to [1] and [2]), it determines if the HAT used cdma2000 1x access network authentication credentials and the CAVE algorithm to create its CHAP response. If the HAT used cdma2000 1x access network authentication credentials and the CAVE algorithm to create the CHAP response, then the home AN-AAA authenticates the HAT using the HAT's cdma2000 1x access network authentication credentials and the CAVE algorithm. If the home AN-AAA cannot authenticate the HAT independently, it communicates with the Home Location Register / Authentication Center (HLR/AC) to authenticate the HAT.

## 1.2 Document Convention

---

“Shall” and “shall not” identify requirements to be followed strictly to conform to the standard and from which no deviation is permitted. “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or (in the negative form) that a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the standard. “Can” and “cannot” are used for statements of possibility and capability, whether material, physical, or causal.

---

<sup>1</sup> cdma2000<sup>®</sup> is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000<sup>®</sup> is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

## 1.3 Normative References

---

For ease of cross referencing, the 3GPP2 references references provided in section 1.3.1 are aligned with the Telecommunications Industry Association (TIA) / Electronics Industry Association (EIA), provided in section 1.3.2.

### 1.3.1 3GPP2

---

- [1] 3GPP2 A.S0007-A v2.0, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces - Rev A*, May 2003.
- [2] 3GPP2 A.S0008-0 v3.0, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces*, May 2003.
- [3] 3GPP2 C.S0023-0 v4.0, *Removable User Identity Module for Spread Spectrum Systems*, June 2001.
- [4] 3GPP2 C.S0023-A v2.0, *Removable User Identity Module for Spread Spectrum Systems*, January 2004.
- [5] 3GPP2 C.S0023-B v1.0, *Removable User Identity Module for Spread Spectrum Systems*, May 2004.
- [6] 3GPP2, S.S0053, *Common Cryptographic Algorithms*, January 2002.
- [7] 3GPP2 X.S0004-E v1.0, *Wireless Radiotelecommunications Intersystem Operations*, March 2004.

### 1.3.2 TIA/EIA

---

- [1] TIA-1878, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces - Alternative Architecture*, May 2003.
- [2] TIA-878-1, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces - Addendum 1*, May 2003.
- [3] TIA/EIA/IS-820-1, *Removable User Identity Module (R-UIM) for TIA/EIA Spread Spectrum Systems, Addendum 1*, June 2001.
- [4] TIA-820-A-1, *Removable User Identity Module for Spread Spectrum Systems - Addendum 1*, April 2004.
- [5] TIA-820-B, *Removable User Identity Module for Spread Spectrum Systems (2004)*, May 2004.
- [6] *Common Cryptographic Algorithms, Revision D.1, September 2000*. An Export Administration Regulations controlled document subject to restricted distribution. Contact the Telecommunications Industry Association, Arlington, VA.
- [7] TIA-41-E, *Wireless Radiotelecommunications Intersystem Operations*, March 2004.

### 1.3.3 Other

---

- [8] Internet Engineering Task Force RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, August 1996.
- [9] Internet Engineering Task Force RFC 2486, *The Network Access Identifier*, January 1999.
- [10] Internet Engineering Task Force RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, June 2000.

## 1.4 Terminology

---

### 1.4.1 Acronyms

---

<b>Acronym</b>	<b>Meaning</b>
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization, and Accounting
AC	Authentication Center
AN	Access Network
ANSI	American National Standards Institute
AT	Access Terminal
AUTHR	Authentication Response
AUTHREQ	AuthenticationRequest INVOKE (refer to [7])
authreq	AuthenticationRequest RETURN RESULT (refer to [7])
CAVE	Cellular Authentication and Voice Encryption
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
HAT	Hybrid MS/AT
HLR	Home Location Register
HRPD	High Rate Packet Data
IMSI	International Mobile Subscriber Identity
LCP	Link Control Protocol
MS	Mobile Station
NAI	Network Access Identifier
PCF	Packet Control Function
PPP	Point-to-Point Protocol
R-UIM	Removable User Identity Module
TIA	Telecommunications Industry Association
UATI	Unicast Access Terminal Identifier
VLR	Visitor Location Register

### 1.4.2 Definitions

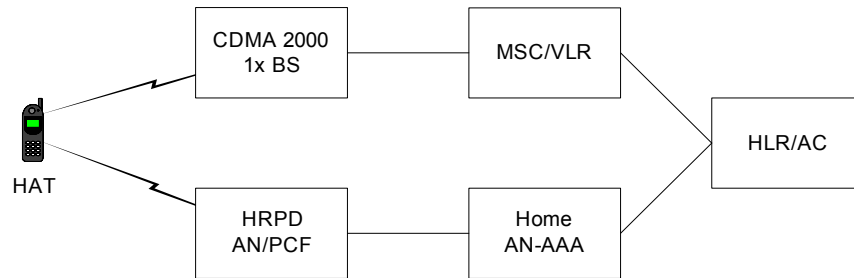
---

AN-AAA	An entity that performs access authentication and authorization functions for the HRPD access network.
cdma2000 1x access network credentials	The set of parameters stored on a R-UIM used to perform ANSI-41 authentication procedures (refer to [3], [4] and [5]).
Hybrid MS/AT	A device capable of operating on both cdma2000 1x and HRPD access networks.

## 1.5 Reference Model

---

Figure 1.5-1 shows the Architecture Reference Model for a HAT that uses its cdma2000 1x access network authentication credentials and algorithm with HRPD network access authentication.



**Figure 1.5-1 Reference Architecture for HAT Authentication**

## 1.6 Assumptions

---

The following assumptions are made regarding HAT and AN/PCF behavior.

1. The operator has configured or used other implementation specific means to instruct the HAT to use cdma2000 1x access network authentication credentials and the CAVE algorithm when performing HRPD network access authentication.
2. When HRPD network access authentication is invoked, the HAT has an inserted R-UIM that contains cdma2000 1x access network authentication credentials.
3. The home AN-AAA can determine whether or not the HAT is using cdma2000 1x access network authentication credentials and the CAVE algorithm when performing HRPD network access authentication.
4. The home AN-AAA communicates with the HLR/AC to authenticate the HAT when the home AN-AAA cannot independently authenticate a HAT that is using cdma2000 1x access network authentication credentials and the CAVE algorithm. The interface between the AN-AAA and HLR/AC is based on [7].

## 2 HAT HRPD Network Access Authentication Using the CAVE Algorithm

---

The following describes the requirements that allow the HAT to use its cdma2000 1x access network authentication credentials and the CAVE algorithm when accessing an HRPD network. This feature extends the access authentication feature described in [1] and [2]. All requirements pertaining to access authentication in [1] and [2] shall be followed except where specifically changed in the following sections.

### 2.1 HAT Requirements

---

The following requirements apply to a HAT that is configured to use its cdma2000 1x access network credentials and the CAVE algorithm for HRPD network access authentication.

The HAT shall perform the following when it receives a CHAP challenge from the AN/PCF:

- The HAT shall execute the Run CAVE function on its R-UIM as described in [3], [4] and [5] using the following input parameters:
  - RANDTYPE shall be set to RAND (global random challenge), and
  - RAND shall be set to the most significant 32 bits of the Value field in the CHAP challenge it received from the AN/PCF. If there are fewer than 32 bits in the Value field, the HAT shall append '0' bits until the number of bits equals 32.
  - AUTH\_DATA shall be set to IMSI\_S1.
- The HAT shall execute the Get Response function as described in [3], [4] and [5] to retrieve the Authentication Response (AUTHR) result of the Run CAVE function and shall place the AUTHR result in the first 3 octets of the Value field in the CHAP response. The HAT shall zero fill the remaining 13 octets of the Value field.
- The HAT shall insert its identification in the form of 'username@realm', according to [9], in the Name field in the CHAP response. The HAT should use as part of its identification an R-UIM-resident component that is associated with the HAT's cdma2000 1x access network credentials. This assists the AN-AAA to determine that the HAT used its cdma2000 1x access network credentials and the CAVE algorithm.
- The HAT shall send the CHAP response to the AN/PCF.

If the HAT cannot successfully execute the Run CAVE or Get Response functions, or there is no R-UIM inserted when the HRPD CHAP challenge is received from the AN/PCF, the HAT should not return a CHAP response to the AN/PCF<sup>2</sup>.

### 2.2 AN/PCF Requirements

---

In an HRPD network that complies with [2], HRPD network access CHAP is used between the AN and HAT. For an HRPD network that complies with [2], there are no additional or modified AN requirements.

In an HRPD network that complies with [1], HRPD network access CHAP is used between the PCF and HAT. For an HRPD network that complies with [1], there are no additional or modified PCF requirements.

### 2.3 Home AN-AAA Requirements

---

This section applies to the home AN-AAA. In this section, all requirements and references to the AN-AAA apply to the home AN-AAA.

---

<sup>2</sup> Note that this requirement overrides the requirement in [8] to send a CHAP response whenever a CHAP challenge is received.

1 The operator may configure the AN-AAA to support HRPD network access authentication. The operator  
2 may configure this support for some HATs or for all HATs.

3 The AN-AAA shall support disabling HRPD network access authentication for a HAT. If the AN-AAA  
4 does not perform HRPD network access authentication for a HAT, the AN-AAA shall send an A12  
5 Access-Accept to the AN/PCF when it receives an A12 Access-Request for the HAT.

6 The operator may configure the AN-AAA to support use of cdma2000 1x access network credentials and  
7 the CAVE algorithm with HRPD network access authentication. The operator may configure this support  
8 for some HATs or for all HATs.

9 The following requirements apply if the operator has configured the AN-AAA to support use of  
10 cdma2000 1x access network credentials and the CAVE algorithm with HRPD network access authent-  
11 ication.

12 When the AN-AAA receives an A12 Access-Request, it shall determine whether the HAT used its  
13 cdma2000 1x access network credentials and the CAVE algorithm to compute the CHAP response. If the  
14 HAT used its cdma2000 1x access network credentials and the CAVE algorithm, the AN-AAA shall  
15 extract the RAND and the AUTHR from the A12 Access-Request. The AN-AAA may identify the HAT's  
16 International Mobile Subscriber Identity (IMSI) from the A12 Access-Request.

17 The AN-AAA shall authenticate the HAT. Authentication can involve the exchange of messages between  
18 the AN-AAA and the HLR/AC. Annex A provides an example of the message exchange between an AN-  
19 AAA and the HLR/AC. If the AN-AAA exchanges messages with the HLR/AC, it shall operate as a  
20 Visitor Location Register (VLR) and support the messages and procedures required to perform MS auth-  
21 entication as defined in [7].

22 If the authentication is successful, the AN-AAA shall send an A12 Access-Accept to the AN/PCF as  
23 described in [1] and [2].

24 If the authentication fails, the AN-AAA shall send an A12 Access-Reject to the AN/PCF. Once authenti-  
25 cation for a HAT has failed a configurable number of times, the AN-AAA may send an A12 Access-  
26 Reject to the AN/PCF when it receives an A12 Access-Request for the HAT.

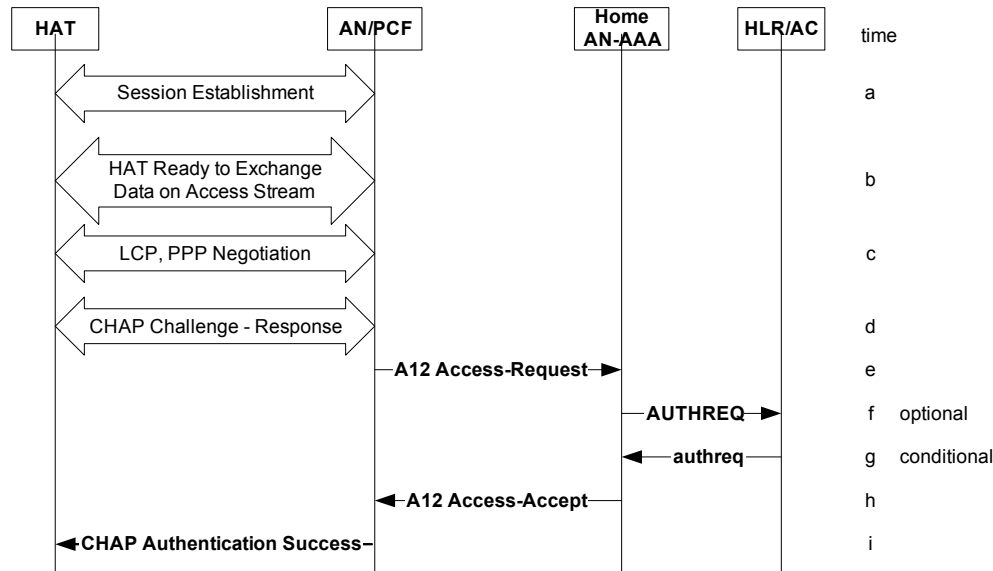
27

28

## Annex A Message Exchange Example

The following provides an example of a message exchange between the home AN-AAA and HLR/AC. An AN-AAA communicates with the HLR/AC when it cannot authenticate the HAT independently.

Figure Annex A-1 shows the overall message flow for HAT authentication in which the exchange of messages between the home AN-AAA and HLR/AC occurs.



**Figure Annex A-1 HAT Authentication Message Flow**

- The HAT and the AN/PCF initiate HRPD session establishment. During this procedure, the AN/PCF does not receive a Unicast Access Terminal Identifier (UATI) for an existing HRPD session. Since no session exists between the HAT and AN/PCF, a session is established where protocols and protocol configurations are negotiated, stored and used for communications between the HAT and the AN/PCF.
- The HAT indicates that it is ready to exchange data on the access stream (e.g., the flow control protocol for the default packet application bound to the AN/PCF is in the open state).
- The HAT and the AN/PCF initiate Point-to-Point Protocol (PPP) and Link Control Protocol (LCP) negotiations for access authentication.
- The AN/PCF generates a random challenge and sends it to the HAT in a CHAP Challenge message in accordance with [8]. The HAT computes and sends its response and identification to the AN/PCF in a CHAP Response message, in accordance with [8]. The CHAP messages carry a global challenge and response.
- When the AN/PCF receives the CHAP response message from the HAT, it sends an Access-Request message on the A12 interface to the AN-AAA which acts as a RADIUS server in accordance with [10]). The AN-AAA determines the HAT used its cdma2000 1x access network credentials and the CAVE algorithm to compute the CHAP response and extracts the RAND and the AUTHR from the A12 Access-Request to authenticate the HAT.
- If the AN-AAA exchanges messages with the HLR/AC, it operates as a VLR and supports the messages and procedures required to perform MS authentication as defined in [7].
- The HLR/AC responds with the (successful) authentication results.
- The AN-AAA sends an Access-Accept message on the A12 interface to the AN/PCF in accordance with [10] (RADIUS).

- 1 i. The AN/PCF returns an indication of CHAP access authentication success to the HAT. Refer to [8].  
 2 In step ‘f’ of Figure Annex A-1, the AuthenticationRequest INVOKE (AUTHREQ) is described in [7].  
 3 The following is an example of how some of the parameters in the AuthenticationRequest INVOKE can  
 4 be set.

<b>Parameter</b>	<b>Contents</b>
ElectronicSerialNumber	Set to the HAT’s identification that was used by the R-UIM for CAVE authentication (refer to [3], [4] and [5]). This can be determined using a local database indexed by the HAT’s identification in the User-Name field in the A12 Access-Request.
MobileIdentificationNumber	Set to the HAT’s MIN. This can be determined using a local database indexed by the HAT’s identification in the User-Name field in the A12 Access-Request.
MSCID	Mobile Switching Center identification. This can be an operator-assigned number not used by any other MSC in the operator’s network.
SystemAccessType	Always set to x’05’ (Page response).
SystemCapabilities	Set to reflect the capability of the AN-AAA and whether SSD should be shared with the AN-AAA.
AuthenticationResponse	Set to the CHAP Response in the CHAP-Password field in the received A12 Access-Request.
RandomVariable	Set to the CHAP Challenge field in the received A12 Access-Request.

- 5 In step ‘g’ of Figure Annex A-1, the AuthenticationRequest RETURN RESULT (authreq) is described in  
 6 [7]. It indicates whether authentication was successful or failed.

7  
 8