

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

3GPP2 S.R0123-0

Version 1.0

Version Date: September 2007



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

## ***Enhanced MMD Security***

### ***Stage 1 Requirements***

---

#### ***COPYRIGHT NOTICE***

*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.*



1

2 **EDITOR**

3 *Scott Marin, Motorola*

4

5 **REVISION HISTORY**

---

6

<b>REVISION HISTORY</b>		
<b>Revision number</b>	<i>Content changes.</i>	<i>Date</i>
0 v1.0	Initial Release	September 2007

1           **Table of Contents**

2

3 Table of Contents ..... ii

4 1 INTRODUCTION ..... 1

5     1.1 INFORMATIVE REFERENCES ..... 1

6     1.2 DEFINITIONS AND ABBREVIATIONS ..... 1

7 2 GENERAL DESCRIPTION..... 3

8 3 HIGH LEVEL REQUIREMENTS ..... 4

9     3.1 System Requirements..... 4

10    3.2 Fixed Network Element Requirements ..... 7

11    3.3 Subscriber Devices..... 7

12    3.4 Security Policy ..... 8

13

1

## 2 **1 INTRODUCTION**

3 This document describes the requirements for security in the  
 4 cdma2000<sup>®1</sup> wireless Internet Protocol (IP) network. The requirements  
 5 are based on leveraging, and extending where applicable, existing  
 6 standard protocols for security.

### 7 **1.1 INFORMATIVE REFERENCES**

- 8  
 9 [1] 3GPP2 X.S0011-D, cdma2000 Wireless IP Network Standard  
 10 [2] 3GPP2 X.S0013-A, Multimedia Domain series, November 2005  
 11 [3] IETF RFC3310, Hypertext Transfer Protocol (HTTP) Digest  
 12 Authentication Using Authentication and Key Agreement (AKA),  
 13 September 2002.  
 14

### 15 **1.2 DEFINITIONS AND ABBREVIATIONS**

16	ACL	Access Control List
17	AKA	Authentication and Key Agreement
18	Anomalous traffic	Traffic which exhibits characteristics that are
19		outside of established boundary values for
20		predefined parameters.
21	Application server	A function that provides all or part of an
22		application level feature or service. An
23		application server may be based on the SIP
24		protocol or on other non-SIP protocols.
25	Baseline traffic	Traffic which has been characterized to establish
26		boundary values for predefined parameters.
27	FW	Firmware
28	HTTP-AKA	Hypertext Transfer Protocol (HTTP) Digest
29		Authentication Using Authentication and Key
30		Agreement (AKA) [3].
31	IDS	Intrusion Detection System
32	IP	Internet Protocol
33	IPS	Intrusion Protection System
34	MMD	Multi-Media Domain

---

<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	Network Element	Network Element is any bearer, signaling, or
2		OAM&P functional entity included within the
3		evolved architecture specifications. Unless
4		specifically excluded, Application Servers are
5		considered within the scope of a Network
6		Element.
7	OAM&P	Operations, Administration, Maintenance, and
8		Provisioning
9	PDN	Packet Data Network
10	QoS	Quality of Service
11	RAN	Radio Access Network
12	Secure Bootstrapping	Secure bootstrapping (e.g., as specified in [1]) is
13		a process by which trusted integrity
14		relationships are enforced during device
15		initialization.
16	Secure Management	Secure management is a process by which the
17		integrity status of a device can be assessed and
18		maintained.
19	Secured Class	A class of Subscriber Devices which can support
20		one or more Subscriber Device requirements
21		defined in this document.
22	Security Assessment	The process of querying a Network Element or
23		Subscriber Device for configuration, Firmware
24		(FW), or Software (SW) status/type, and
25		comparing that information against associated
26		policies.
27	SMS	Short Message Service
28	SW	Software
29	Subscriber Device	Subscriber Device is any device which can
30		communicate with the RAN and/or Core
31		Network.
32	System	Components of the 3GPP2 PDN and MMD
33		network consisting of the Subscriber Device,
34		RAN, and Core Network
35	Policy	A set of rules which control the behavior and/or
36		state of a Network Element or Subscriber Device.

1 **2 GENERAL DESCRIPTION**

2 This document provides high level requirements for Multi-Media Domain  
3 (MMD) Security. It includes basic requirements inherent in existing MMD  
4 specifications [2] plus new requirements that are an addition to or  
5 expand on existing security requirements.

## 1 **3 HIGH LEVEL REQUIREMENTS**

### 2 **3.1 System Requirements**

3 System requirements span fixed Network Elements in the Core Network,  
4 Radio Access Network (RAN), and Subscriber Devices. These elements are  
5 collectively referred to as “the system.” The following system  
6 requirements are intended to cover all aspects of service delivery,  
7 including home-network and visited-network scenarios.

8 **SYS001** – The system shall support secure bootstrapping and secure  
9 management of Network Elements and Subscriber Devices.

10 **SYS002** – The system shall provide resistance against denial-of-service  
11 attacks to, and through, its Network Elements.

12 **Note:** A denial-of-service attack comprises any detectable service  
13 interruption or system performance degradation. The scope includes  
14 denial-of-service attack scenarios from wired and wireless nodes.

15 **SYS003** – The system shall be capable of querying a Subscriber Device  
16 for information such as device status and hardware and software  
17 configurations.

18 **SYS004** – The system may request quarantine functions based on the  
19 security assessment and policy for the Subscriber Devices.

20 **SYS005** - The system may request remediation functions based on the  
21 security assessment and policy for the Subscriber Devices.

22 **SYS006** – The system shall support standardized protocols to facilitate  
23 the generation of security alarms and incident reports to one or more  
24 collection points.

25 **SYS007** – The system shall support the capability for a centralized  
26 security control point to monitor, process, and provide notification of  
27 security events of all of the Network Elements.

28 **SYS008** – The system shall support capabilities for correlation of  
29 security events, analysis of real-time events, and flow reporting  
30 performed by Network Elements in support of an Intrusion Detection  
31 System (IDS) and an Intrusion Prevention System (IPS).

32 **Note:** Although IDS/IPS functions may be covered by Operations,  
33 Administration, Maintenance, and Provisioning (OAM&P) specifications,  
34 this requirement ensures that information needed to support the  
35 IDS/IPS functions (e.g., Quality of Service (QoS) flow parameters) shall be  
36 included in the standard specifications.

1 **SYS009** – The system shall support a security policy framework. As an  
2 example, a security policy may contain a set of rules that determines  
3 which Network Element protects a given traffic type, what kind of  
4 protection will be used, how often rekeying will occur, and parameters  
5 associated with Network Element compliance.

6 **SYS010** – The system shall support capabilities to identify anomolous  
7 traffic.

8 **SYS011** – The system shall support capabilities to filter anomolous or  
9 malicious traffic .

10 **SYS012** – The system shall support capabilities to support security  
11 associations with trusted entities (such as partner application servers,  
12 and roaming partners).

13 **SYS013** – The system shall support capabilities for operator policies to  
14 govern the reporting of security events.

15 **SYS014** – The system shall support capabilities for operator policies to  
16 govern responses to specified security events. Examples of such  
17 responses are:

- 18 • install or update Access Control Lists (ACLs),
- 19 • de-authorize connections with a Network Element,
- 20 • force a Network Element to upgrade its software,
- 21 • de-authorize specific services,
- 22 • send an Short Message Service (SMS) message to specific users.

23 **SYS015** – The system shall enable separate administrative domains for  
24 each system component, including:

- 25 • Subscriber Device,
- 26 • Access Network components (visited or home),
- 27 • Core Network components (home or transit),
- 28 • Application Servers (visited, home, 3<sup>rd</sup> party).

29 **SYS016** – The system shall support the capability for operators to  
30 manage independent security policies for their respective system  
31 components.

32 **SYS017** – The system shall support mutual authentication between the  
33 Subscriber Device and the network (e.g., authentication server).

34 **SYS018** – The system shall support the capability to authorize each  
35 Network Element before it is allowed to send IP traffic through the  
36 system.

1 **SYS019** – The system shall support access network independent  
2 authentication mechanisms for Subscriber Devices.

3 **Note:** This covers both intra-system and inter-system interfaces.

4 **SYS020** – The system shall support mutual authentication between any  
5 two communicating Network Elements.

6 **Note:** This covers both intra-system and inter-system interfaces.

7 **SYS021** – The system shall provide the capability to prevent  
8 unauthorized users from accessing the system based on operator policy.

9 **SYS022** – The system shall provide the capability to apply and verify the  
10 integrity and confidentiality protections of bearer and control traffic on  
11 all standardized interfaces within the service provider’s network, and  
12 with peered networks, based on operator policy.

13 **SYS023** – The system shall support the ability to secure data traversing  
14 network paths. Note that this is usually accomplished through replay,  
15 fraud, encryption, and integrity protection methods.

16 **SYS024** – The system shall support data origin authentication for  
17 signaling messages using integrity protection of signaling messages  
18 between the signaling endpoints.

19 **SYS025** – The system shall provide the capability for subscriber  
20 authentication and service authorization (i.e., grant use of system  
21 resources) based on operator policy.

22 **SYS026** – The system security mechanisms shall enable policy-driven  
23 controls to account for tradeoffs, e.g., network resource consumption vs.  
24 user experience degradation.

25 **SYS027** – The system shall provide the capability to support a repository  
26 for security related data (including identity and credential management).

27 **SYS028** – The system shall use industry-validated mechanisms for  
28 strong cryptography and random number generation.

29 **SYS029** –The system shall support communication through firewalls.  
30 Firewalls shall not prevent authorized data sessions to/from Subscriber  
31 Devices.

32 **SYS030** – The system should minimize over-the-air transactions for  
33 Subscriber Devices which are capable of multiple authentication, key  
34 generation, and key distribution mechanisms. As an example, a subset of  
35 authentication mechanisms could be applied to multiple protocol layers  
36 (link, network, transport Layer, or application layers).

1 **SYS031** – The system should minimize over-the-air overheads for  
2 Subscriber Devices which are capable of supporting multiple integrity  
3 and confidentiality mechanisms. As an example, a subset of those  
4 mechanisms could be applied across multiple protocol layers (link,  
5 network, transport layer, or application layers).

6 **SYS032** – The system shall support the capability for each Network  
7 Element to implement admission control (e.g., during the connection  
8 establishment phase) for all standardized interfaces.

9 **SYS033** – The system shall support the capability for service  
10 authorization based on availability of network resources (e.g., bandwidth,  
11 traffic type, operator policy, and the subscriber profile).

### 12

### 13 **3.2 Fixed Network Element Requirements**

14 **SYS034** – Protocols supporting Network Element interfaces shall protect  
15 against host intrusion.

16 **SYS035** –Network Elements must be able to protect its resources and  
17 applications against viruses and worms.

### 18

### 19 **3.3 Subscriber Devices**

20 **SYS036** – Subscriber Devices shall support integrity protection of  
21 signaling messages with the entity that terminates the signaling.

22 **SYS037** - Secured classes of a Subscriber Device shall include  
23 mechanism which can continuously monitor and dynamically report  
24 device security status.

25 **SYS038** - Secured classes of a Subscriber Device shall include  
26 mechanism which can allow the access network to assess the device  
27 security status.

28 **SYS039** - Secured classes of a Subscriber Device shall report security  
29 status for purposes of admission control and remediation.

30 **SYS040** - Secured classes of a Subscriber Device shall include  
31 mechanism which can prevent it from sourcing malicious traffic into the  
32 access network.

33 **SYS041** - Secured classes of a Subscriber Device shall support receiving  
34 configuration settings from an authenticated Network Element via  
35 network controlled policy configuration.

36

1 **3.4 Security Policy**

2 **SYS042** – In roaming and peering contexts, security policy shall  
3 determine which asserted user identities can be exported by the system  
4 to other networks.

5 **SYS043** – The security policy framework shall support compliance level  
6 assessment and associated actions.

7 **SYS044** – Any ‘out of compliance’ Network Elements shall trigger  
8 security event reporting.

9