

RR6-2 Acknowledgment of a Conflict Resolution for a Subscription Version

NPAC SMS shall acknowledge receiving a conflict resolution request for a Subscription Version via the SOA to NPAC SMS Interface.

RR6-3 Deferred Disconnect of a Subscription Version

NPAC SMS shall allow a specific Subscription Version to be placed into a deferred disconnect status by having the effective date in the future via the SOA to NPAC SMS Interface.

RR6-4 Cancel Request Notification

NPAC SMS shall notify a Service Provider of a request for a Subscription Version status to be changed to cancel via the SOA to NPAC SMS Interface.

RR6-5 Conflict Resolution Request Notification

NPAC SMS shall notify a Service Provider of a request for a Subscription Version status to be changed to conflict resolution via the SOA to NPAC SMS Interface.

RR6-6

(Duplicate - refer to R10-10.1)

RR6-7

(Duplicate - refer to R10-10.1)

6.4.4 Request Restraints

RR6-8 Tunable Parameter Number of Aggregated Download Records

NPAC SMS shall allow NPAC System Administrators to specify a tunable parameter value for the maximum number of download records.

RR6-9 Download Time Tunable Parameter to Restricted Time Range

NPAC SMS shall allow NPAC System Administrators to specify a tunable parameter value for the maximum time range for a download.

RR6-10

DELETE

RR6-11

(Duplicate - refer to RX6-2.5)

RR6-12

DELETE (moved to RX6-2.6)

RR6-13 Queries Constrained by NPA-NXX

NPAC SMS shall constrain all queries on the NPAC SMS to Local SMS Interface to one NPA-NXX plus additional filter criteria.

6.5 NPAC SOA Low-tech Interface

The NPAC SOA Low-tech Interface supports the request functionality of the SOA to NPAC SMS interface.

RX6-2.1 NPAC SOA Low-tech Interface

NPAC SMS shall provide an NPAC SOA Low-tech Interface.

RX6-2.2 SOA to NPAC SMS Create Subscription Versions administration requests via an NPAC SOA Low-tech Interface

NPAC SMS shall support Create Subscription Version requests via a secure, NPAC SOA Low-tech Interface.

RX6-2.3 SOA to NPAC SMS Cancel Subscription Versions administration requests via an NPAC SOA Low-tech Interface

NPAC SMS shall support Cancel Subscription Version requests via a secure, NPAC SOA Low-tech Interface.

RX6-2.4 SOA to NPAC SMS Modify Subscription Versions administration requests via an NPAC SOA Low-tech Interface

NPAC SMS shall support Modify Subscription Version requests via a secure, NPAC SOA Low-tech Interface.

RX6-2.5 SOA to NPAC SMS Query Subscription Versions administration requests via an NPAC SOA Low-tech Interface

NPAC SMS shall support query of Subscription Versions via a secure, NPAC SOA Low-tech Interface.

RX6-2.6 SOA to NPAC SMS Activate Subscription Versions administration requests via an NPAC SOA Low-tech Interface

NPAC SMS shall support Activation of Subscription Versions via a secure, NPAC SOA Low-tech Interface.

RX6-2.7 SOA to NPAC SMS Disconnect Subscription Versions administration requests via an NPAC SOA Low-tech Interface

NPAC SMS shall allow NPAC personnel and users of the SOA to NPAC SMS interface to request disconnection of a Subscription Version via a secure, NPAC SOA Low-tech Interface.

RX6-3 SOA to NPAC SMS audit requests

NPAC SMS shall support SOA to NPAC SMS audit requests for all, part or one Service Provider via the NPAC SOA Low-tech Interface.

RX6-3.1

DELETE

RX6-4 NPAC SMS Notification Handling

NPAC SMS shall support, via a secure NPAC SOA Low-tech Interface, a method to view and locally capture notifications that have occurred for the service provider upon request.

7. Security

7.1 Overview

In addition to the general security requirements based on the user interface paradigm in Section 7.2 through 0, there are requirements for the security on an OSI application to application interface (such as the one specified in Section 6, *NPAC SMS Interfaces*, for the SMS to SMS and SMS to SOA interfaces).

7.2 Identification

The NPAC will accept only authorized NPAC customers through interface connections, and among NPAC customers, the NPAC will make appropriate limitations on their actions (for example, letting only old or new Service Providers view a pending record). The NPAC will only accept authorized customer user IDs. However, the NPAC will make no distinction among an NPAC customer's employees; the NPAC customer and their systems must control individual NPAC customer employee actions.

A user identification is a unique, auditable representation of the user's identity within the system. The NPAC SMS requires all system users, both individuals and remote machines, to be uniquely identified to support individual accountability over the NPAC Administrative and NPAC SOA Low-tech Interfaces.

R7-1 Unique User Identification Codes - Individuals

NPAC SMS shall require unique user identification codes (userid) to identify all NPAC and Service Provider personnel.

R7-2 Assigned Userid Identification

NPAC SMS shall require NPAC and Service Provider personnel to identify themselves with their assigned userid before performing any actions.

R7-3 Current Active User List Maintenance

NPAC SMS shall maintain internally the identity of all NPAC and Service Provider personnel logged on to the NPAC SMS.

R7-4 User Invoked Processes

NPAC SMS shall have for every process running an associated userid of the invoking user (or the userid associated with the invoking process).

R7-5.1 Userids, Unused - Disabling

NPAC SMS shall disable userids after a period of time during which the userId has not been used.

R7-5.2 Unused Userid Disable Period - Tunable Parameter

NPAC SMS shall provide an Unused Userid Disable Period tunable parameter which is defined as the number of days for which the userId has not been used.

R7-5.3 Unused Userid Disable Period - Tunable Parameter Modification

NPAC SMS shall allow the NPAC SMS administrator to modify the Unused Userid Disable Period tunable parameter time period.

R7-5.4 Unused Userid Disable Period - Tunable Parameter Default

NPAC SMS shall default the Unused Userid Disable Period tunable parameter to 60 days.

R7-6.1 Userids, Disabled - Reinstatement

NPAC SMS shall provide a complementary mechanism or procedure for the re-instatement disabled userids.

R7-6.2 Userids - Deletion

NPAC SMS shall provide a procedure for the deletion of userids.

R7-7 Userids - Temporary Disabling

NPAC SMS shall support the temporary disabling of userids.

R7-8 Userids, Disabled - Automatic Reactivation

NPAC SMS shall provide an option for automatic reactivation of disabled userids.

R7-9.1 Userids - One Active Login

NPAC SMS shall control and limit simultaneous active usage of the same userids by allowing only one active login.

R7-9.2 Second Login Attempt

NPAC SMS shall present the NPAC or Service Provider personnel with an option of disconnecting the first login and continuing the second login or terminating the second login, when a second login is entered.

7.3 Authentication

The identity of all NPAC SMS system users, both individuals and remote machines, must be verified or authenticated to enter the system, and to access restricted data or transactions over the NPAC Administrative and NPAC SOA Low-Tech Interfaces.

R7-10 User Authentication

NPAC SMS shall authenticate the identity of all NPAC and Service Provider users of the NPAC Administrative and NPAC SOA Low-tech Interfaces prior to their initially gaining access to NPAC SMS.

R7-11

(Duplicate - refer to R7-10)

R7-12 Authentication Data Protection

NPAC SMS shall protect all internal storage of authentication data so that it can only be accessed by an NPAC Security Administrator user.

7.3.1 Password Requirements

R7-13 Passwords - Non-shared

NPAC SMS shall require a single password entry for each userID.

R7-14 Passwords - Userid Unique

NPAC SMS shall allow a user to define a password that is already associated with another userID.

R7-15 Passwords - One-Way Encrypted

NPAC SMS shall store passwords in a one-way encrypted form.

R7-16 Passwords, Encrypted - Privileged Users Access Control

NPAC SMS shall only allow access to encrypted passwords by authorized users.

R7-17

(Duplicate - refer to R7-15)

R7-18 Passwords, Entry - Automatic Clear Text Suppression

NPAC SMS shall automatically suppress or fully blot out the clear-text representation of the password on the data entry device.

R7-19 Passwords - Network Transmission Clear Text Suppression

NPAC SMS shall ensure that passwords sent over public or external shared data networks are encrypted.

R7-20 Passwords - Non-Null

NPAC SMS shall require non-null passwords.

R7-21 Passwords - User-Changeable

NPAC SMS shall provide a mechanism to allow passwords to be user-changeable. This mechanism shall require re-authentication of the user identity.

R7-22 Passwords - Reset Capability

The NPAC SMS shall have a mechanism to reset passwords.

R7-23.1 Passwords - Aging Enforcement

NPAC SMS shall enforce password aging.

R7-23.2 Password Aging Default

NPAC SMS shall default the system password aging to 90 days.

R7-24.1 Passwords - Expiration Notification

NPAC SMS shall notify users a NPAC-specifiable period of time prior to their password expiring. The system supplied default shall be seven days.

R7-24.2 Passwords - Expiration Notification Default

NPAC SMS shall default the password expiration notification time period to seven days

R7-24.3 Passwords - Require User to Enter New Password

NPAC SMS shall require any user whose password has expired to enter a new password before allowing that user access to the system.

R7-25.1 Passwords - Non-Reusable

NPAC SMS shall ensure that a password can not be reused by the same individual for specifiable period of time.

R7-25.2 Password Reuse Default

NPAC SMS shall default the time period in which a password can not be reused to six months.

R7-26.1 Passwords - Minimum Structure Standard #1

Passwords shall contain a combination of at least six case-sensitive alphanumeric characters including at least one alphabetic and one numeric or punctuation character.

R7-26.2 Passwords - Associated Userid

NPAC SMS shall ensure that passwords do not contain the associated userId.

R7-27.1 Password Generator

NPAC SMS shall provide a password generator.

R7-27.2 Passwords, System Generated - Attack Resistant

NPAC SMS shall ensure that generated passwords are "reasonably" resistant to brute-force password guessing attacks.

R7-27.3 Passwords, System Generated - Random

NPAC SMS shall ensure that the generated sequence of passwords have the property of randomness.

7.4 Access Control

Access to the NPAC SMS and other resources will be limited to those users that have been authorized for that specific access right.

7.4.1 System Access

R7-28.1 System Access - Individuals

NPAC SMS shall allow access to authorized individual users.

R7-28.2 System Access - Remote Machines

NPAC SMS shall allow access to authorized remote systems.

R7-29.1 System Access, User Information - Entry

NPAC SMS shall provide a facility for the initial entry of authorized user and associated authentication information.

R7-29.2 System Access, User Information - Modification

NPAC SMS shall provide a facility for the modification of authorized user and associated authentication information.

R7-30

(Duplicate - refer to R7-10)

R7-31 System Access, Login - Trusted Communication

NPAC SMS's login procedure shall be able to be reliably initiated by the user, i.e., a trusted communications path should exist between NPAC SMS and the user during the login procedure.

R7-32.1 System Access - Disconnect User

NPAC SMS shall disconnect end users after a period of non-use.

R7-32.2 Non-use Disconnect Tunable Parameter

NPAC SMS shall default the Non-use Disconnect tunable parameter to 60 minutes.

R7-33.1 System Access - User Authentication Failure

NPAC SMS shall exit and end the session if the user authentication procedure is incorrectly performed a specifiable number of times.

R7-33.2 Incorrect Login Exit Default

NPAC SMS shall default the number of allowable incorrect login attempts to 3.

R7-34 System Access, User Authentication Failure - Notification

NPAC SMS shall provide a mechanism to immediately notify the NPAC SMS system administrator when the threshold in R7-33.1 is exceeded.

R7-35.1 System Access - Login Process I/O Port Restart

NPAC SMS shall restart the login process when the threshold in R7-33.1 has been exceeded and a specified interval of time has passed.

R7-35.2 Login Process Restart Default

NPAC SMS shall default the time interval to restart the login process to 60 seconds.

R7-36 System Access, User Authentication Failure - Userid Non-Suspension

NPAC SMS shall not suspend the userId upon exceeding the threshold in R7-33.1.

R7-37 System Access, User Authentication Procedure - Entry

NPAC SMS shall perform the entire user authentication procedure even if the userId that was entered was not valid.

R7-38 System Access, User Authentication Procedure Entry - Error Feedback

NPAC SMS shall only provide error feedback of "invalid".

R7-39 System Access, User Authentication Procedure Entry - Time Parameters

NPAC SMS shall provide a mechanism to restrict user login based on time-of-day, day-of-week, calendar date.

R7-40.1 System Access, User Authentication Procedure Entry - Method

NPAC SMS shall provide a mechanism to restrict user login based on method of entry.

R7-40.2 System Access, User Authentication Procedure Entry - Location

NPAC SMS shall provide a mechanism to restrict user login based on user system location.

R7-41 System Access, User Authentication Procedure Entry - Dial-Up Limitations

NPAC SMS shall provide a mechanism to limit the users authorized to access the system via dial-up facilities.

R7-42.1 System Access - Network Basis

NPAC SMS shall provide a mechanism to limit system entry for privileged NPAC SMS users on a specifiable network access.

R7-42.2 System Access - Per-Port Basis

NPAC SMS shall provide a mechanism to limit system entry for privileged NPAC SMS users on a specifiable per-port basis.

R7-43.1 System Access, Network Authentication

NPAC SMS shall provide a strong authentication mechanism for network access.

R7-43.2 Internet Access

NPAC SMS shall use authentication of public encryption keys for users accessing the NPAC SMS over the Internet.

R7-43.3 Dial-in Access

NPAC SMS shall use smart cards to authenticate users accessing the NPAC SMS via dial-up.

R7-44 System Access - Secure Logoff Procedures

NPAC SMS shall provide a mechanism to end the session through secure logoff procedures.

R7-45

(Duplicate - refer to R7-47)

R7-46 System Access, Unauthorized Use Message - Specifiable

NPAC SMS shall ensure that the message is NPAC SMS-specifiable to meet their own requirements, and any applicable laws.

R7-47.1 System Access, Unauthorized Use Message - Specifiable

NPAC SMS shall be able to display an advisory warning message of up to 20 lines in length prior to login.

R7-47.2 Advisory Warning Message Default

NPAC SMS shall default the pre-login advisory warning message to the following:

**NOTICE: This is a private computer system.
Unauthorized access or use may lead to prosecution.**

R7-48.1 System Access - User's Last Successful Access

NPAC SMS shall display the date and time of the user's last successful system access upon successful login.

R7-48.2 System Access - User's Unsuccessful Access Attempts

NPAC SMS shall display the number of unsuccessful attempts by that userId to access the system, since the last successful access by that userId upon successful login.

R7-49.1 System Access, Security Administration - Authorize Users

NPAC SMS shall only allow the NPAC Security Administrator to authorize users.

R7-49.2 System Access, Security Administration - Revoke Users

NPAC SMS shall only allow the NPAC Security Administrator to revoke users.

R7-50.1 System Access, Security Administration - Adding Users

NPAC SMS shall provide security documentation that defines and describes procedures for adding users.

R7-50.2 System Access, Security Administration -Deleting Users

NPAC SMS shall provide security documentation that defines and describes procedures for deleting users.

7.4.2 Resource Access

R7-51 Data Access for Authorized Users

NPAC SMS shall allow only authorized users to access the data that is part of or controlled by the SMS system.

R7-52 Service Provider Data Protected

NPAC SMS shall protect service provider data from access by unauthorized users.

R7-53.1 Authorized User Access to Software

NPAC SMS shall ensure that only NPAC system administrators can access the software files that constitutes the NPAC SMS.

R7-53.2 Authorized User Access to Transactions

NPAC SMS shall ensure that only authorized users can access the transactions that constitute the NPAC SMS.

R7-53.3 Authorized User Access to Data

NPAC SMS shall ensure that only authorized NPAC Administrative and NPAC SOA Low-tech Interfaces users can access the data generated by the transactions that constitutes the SMS.

R7-54.1 Access Control of Executable Software

NPAC SMS shall ensure that the executable and loadable software is access controlled for overwrite and update, as well as execution rights.

R7-55 Access Control of Resources

NPAC SMS shall ensure that control of access to resources is based on authenticated user identification.

R7-56 Use of Encryption

NPAC SMS shall ensure that userId and password is used as a primary access control for direct login and system ID is used for primary access control to the SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface.

R7-57 Resource Access to Users

NPAC SMS shall ensure that for software resources controlled by NPAC SMS, it must be possible to grant access rights to a single user or a group of users.

R7-58 Resource Access Denied to Users

NPAC SMS shall ensure that for software resources controlled by NPAC SMS, it must be possible to deny access rights to a single user or a group of users.

R7-59

(Duplicate - refer to R7-53.3)

R7-60 Only NPAC Personnel Can Modify User Access

NPAC SMS shall allow only NPAC personnel to modify access rights to a resource.

R7-61 Removal of User Access Rights

NPAC SMS shall provide a mechanism to remove access rights to all software resources for a user or a group of users.

R7-62.1

(Duplicate - refer to R7-12)

R7-62.2

(Duplicate - refer to R7-12)

7.5 Data and System Integrity

R7-63 Identify Originator of System Resources

NPAC SMS shall identify the originator of any accessible system resources.

R7-64 Identify Originator of Information Received Across Communication Channels

NPAC SMS shall be able to identify the originator of any information received across communication channels.

R7-65.1 Monitor System Resources

NPAC SMS NMS shall use SNMP to monitor the system resources.

R7-65.2 Detect Error Conditions

NPAC SMS NMS shall use SNMP to detect error conditions.

R7-65.3 Detect Communication Errors

NPAC SMS NMS shall use SNMP to detect communication errors.

R7-65.4 Detect Link Outages

NPAC SMS NMS shall use SNMP to detect link outages.

R7-66.1 Rule Checking on Update

NPAC SMS shall ensure proper rule checking on data update.

R7-66.2 Handling of Duplicate Inputs

NPAC SMS shall handle duplicate/multiple inputs.

R7-66.3 Check Return Status

NPAC SMS shall check return status.

R7-66.4 Validate Inputs

NPAC SMS shall validate inputs for reasonable values.

R7-66.5 Transaction Serialization

NPAC SMS shall ensure proper serialization of update transactions.

R7-67 Database Integrity Checking

NPAC SMS shall include database integrity checking utilities for the NPAC SMS database.

7.6 Audit

7.6.1 Audit Log Generation

R7-68.1 Security Audit Log for After the Fact Investigation

NPAC SMS shall generate a security audit log that contains information sufficient for after the fact investigation of loss or impropriety for appropriate response, including pursuit of legal remedies.

R7-68.2 Security Audit Data Availability

NPAC SMS shall ensure that the security audit data is available on-line for a minimum of 90 days.

R7-68.3 Security Audit Data Archived

NPAC SMS shall archive the security audit data off-line for a minimum of two years.

R7-69 User Identification Retained

NPAC SMS shall ensure that the user-identification associated with any NPAC SMS request or activity is maintained, so that the initiating user can be traceable.

R7-70 Protection of Security Audit Log Access

NPAC SMS shall protect the security audit log from unauthorized access.

R7-71.1

DELETE

R7-71.2 NPAC Personnel Delete Security Audit Log

NPAC SMS shall ensure that only authorized NPAC personnel can archive and delete any or all of the security audit log(s) as part of the archival process.

R7-72 Security Audit Control Protected

NPAC SMS shall ensure that the security audit control mechanisms are protected from unauthorized access.

R7-73.1 Log Invalid User Authentication Attempts

NPAC SMS shall write a record to the security audit log for each invalid user authentication attempt.

R7-73.2 Log NPAC SMS End User Logins

NPAC SMS shall write a record to the security audit log for logins of NPAC users.

R7-73.3 Log NPAC Personnel Activities

NPAC SMS shall write a record to the security audit log for security controlled activities of NPAC users.

R7-73.4 Log Unauthorized Data Access

NPAC SMS shall write a record to the security audit log for unauthorized data access attempts.

R7-73.5 Log Unauthorized Transaction Access

NPAC SMS shall write a record to the security audit log for unauthorized NPAC SMS transaction functionality access attempts.

R7-74 No Disable of Security Auditing

NPAC SMS shall ensure that NPAC audit capability cannot be disabled.

R7-75 Security Audit Record Contents

NPAC SMS shall ensure that for each recorded event, the audit log contains the following:

- Date and time of the event
- User identification including relevant connection information
- Type of event
- Name of resources accessed or function performed
- Success or failure of the event

R7-76.1 Recorded Login Attempts

NPAC SMS shall record actual or attempted logins in audit logs after an NPAC-tunable parameter threshold of consecutive login failures.

7.6.2 Reporting and Intrusion Detection

R7-77.1 Exception Reports on Data Items

NPAC SMS shall provide post-collection audit analysis tools that can produce exception reports on items relating to system intrusions.

R7-77.2 Exception Reports on Users

NPAC SMS shall provide post-collection audit analysis tools that can produce exception reports on users relating to system intrusions.

R7-77.3 Exception Reports on Communication Failures

NPAC SMS shall provide post-collection audit analysis tools that can produce exception reports on communication failures relating to system intrusions.

R7-77.4 Summary Reports on Data Items

NPAC SMS shall provide post-collection audit analysis tools that can produce summary reports on data items relating to system intrusions.

R7-77.5 Summary Reports on Users

NPAC SMS shall provide post-collection audit analysis tools that can produce summary reports on users relating to system intrusions.

R7-77.6 Summary Reports on Communication Failures

NPAC SMS shall provide post-collection audit analysis tools that can produce summary reports on communication failures relating to system intrusions.

R7-77.7 Detailed Reports on Data Items

NPAC SMS shall provide post-collection audit analysis tools that can produce detailed reports on data items relating to system intrusions.

R7-77.8 Detailed Reports on Users

NPAC SMS shall provide post-collection audit analysis tools that can produce detailed reports on users relating to system intrusions.

R7-77.9 Detailed Reports on Communication Failures

NPAC SMS shall provide post-collection audit analysis tools that can produce detailed reports on communication failures relating to system intrusions.

R7-78 Review User Actions

NPAC SMS shall provide a capability to review a summary of the actions of any one or more users, including other NPAC users, based on individual user identity.

R7-79.1 Monitor Network Address

NPAC SMS shall provide tools for the NPAC to monitor the message passing activities to and from a specific network address as they occur.

R7-80.1 Real-time Security Monitor

NPAC SMS NMS shall provide a real-time mechanism to monitor the occurrence or accumulation of security auditable events. Where possible, NPAC SMS shall determine and execute the least disruptive action to terminate the event.

R7-80.2 Security Event Notification

NPAC SMS NMS shall notify the NPAC personnel immediately when security event thresholds are exceeded through the SNMP agent.

7.7 Continuity of Service

R7-81 System Made Unavailable by Service Provider

NPAC SMS shall ensure that no service provider action, either deliberate or accidental, should cause the system to be unavailable to other users.

R7-82 Detect Service Degrading Conditions

NPAC SMS shall report conditions that would degrade service below a pre-specified minimum, including high memory, CPU, network traffic, and disk space utilization.

R7-83 System Recovery After Failure

NPAC SMS shall provide procedures or mechanisms to allow recovery after a system failure without a security compromise.

R7-84.1 Software Backup Procedures

NPAC SMS shall have documented procedures for software backup.

R7-84.2 Data Backup Procedures

NPAC SMS shall have documented procedures for data backup.

R7-84.3 Software Restoration Procedures

NPAC SMS shall have documented procedures for software restoration.

R7-84.4 Data Restoration Procedures

NPAC SMS shall have documented procedures for data restoration.

R7-85.1 Software Version Number

NPAC SMS shall record the exact revision number of the latest software installed.

R7-85.2 Software Version Number

NPAC SMS shall display for viewing the exact revision number of the latest software via a Web bulletin board, and also through the NPA Administrative and NPAC SOA Low-tech Interfaces upon completion of the user login sequence.

7.8 Software Vendor

R7-86 Software Development Methodology

NPAC SMS shall be developed using a corporate policy governing the development of software.

R7-87 Bypass of Security

NPAC SMS shall not support any mode of entry into NPAC SMS for maintenance, support, or operations that would violate or bypass any security procedures.

R7-88 Documented Entry

NPAC SMS shall document any mode of entry into the SMS for maintenance, support, or operations.

7.9 OSI Security Environment

7.9.1 Threats

Attacks against the NPAC SMS may be perpetrated in order to achieve any of the following:

- Denial of service to a customer by placing wrong translation information in the SMS
- Denial of service to a customer by preventing a valid message from reaching the SMS
- Disrupting a carrier's operations by having numerous spurious calls (to users who are not clients of that carrier) directed to that carrier
- Switching customers to various carriers without their consent
- Disrupting the functioning of the NPAC SMS by swamping it with spurious messages

7.9.2 Security Services

R7-89 Authentication

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support Authentication (at association setup).

R7-90 Data Origin Authentication

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support data origin authentication for each incoming message.

R7-91.1 Detection of Message Replay

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of replay.

R7-91.2 Deletion of a Message

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of message deletion.

R7-91.3 Modification of a Message

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of message modification.

R7-91.4 Delay of a Message

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of message delay.

R7-92 Non-repudiation of Origin

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support non-repudiation of origin.

R7-93 Access Control

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall allow only authorized parties (i.e., carriers serving a given customer) to cause changes in the NPAC SMS database.

7.9.3 Security Mechanisms

This section outlines the requirements to specify security mechanisms.

7.9.3.1 Encryption

R7-94.1 Public Key Crypto System (PKCS)

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall use a public key crypto system (PKCS) to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms.

R7-94.2 Digital Signature Algorithms

NPAC SMS shall support one of the digital signature algorithms listed in the OIW Stable Implementation Agreement, Part 12, 1995.

R7-95 RSA Encryption Modulus Size

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall require the size of the modulus of each key to be at least 600 bits for RSA encryption.

7.9.3.2 Authentication

R7-96 Digital Signature Algorithm

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall apply the digital signature algorithm to the fields specified below without any separators between those fields or any other additional characters.

- The unique identity of the sender
- The Generalized Time, corresponding to the issuance of the message
- A sequence number
- A key identifier
- Key list ID

R7-97 Authenticator Contents

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall provide authentication consisting of the following:

- The unique identity of the sender
- The Generalized Time, corresponding to the issuance of the message
- A sequence number
- A key identifier
- The digital signature of the sender's identity, Generalized Time and sequence number listed above
- Key list ID

R7-98 Authenticator in Access Control Field

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall convey the authenticator in the CMIP access control field.

7.9.3.3 Data Origin Authentication

R7-99.1 Subsequent Messages Contain Access Control Field

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that every subsequent CMIP message that contains the access control field carries the authenticator.

R7-99.2 Separate Counter for Association Sequence Numbers

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall verify that each party maintains a separate sequence number counter for each association it uses to send messages.

R7-99.3 Increment Sequence Numbers

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall verify that every time the authenticator is used the value of the sequence number will be incremented by one.

7.9.3.4 Integrity and Non-repudiation

R7-100.1 Security Field

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that all the notifications defined for the number portability application contain a security field.

R7-100.2 Security Field Syntax

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that the syntax of the security field used for the notification corresponds to the authenticator.

R7-101.1

DELETE

R7-101.2

(Duplicate - refer to R7-91.1)

R7-101.3

(Duplicate - refer to R7-91.2)

R7-101.4

(Duplicate - refer to R7-91.3)

R7-101.5

(Duplicate - refer to R7-91.4)

R7-102 Notifications in Confirmed Mode

NPAC SMS shall ensure that all the notifications are sent in the confirmed mode.

R7-103

MISSING in RFP

7.9.3.5 Access Control

R7-104 Responsible for Access Control

NPAC SMS shall be responsible for access control on the SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface.

R7-105.1

(Duplicate - refer to R7-97 and R7-98)

R7-105.2 Generalized Time

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that external messages received have a generalized time in the access control information within 5 minutes of the NPAC SMS system clock.

7.9.3.6 Audit Trail

R7-106 Log Contents

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall keep a log of all of the following:

- Incoming messages that result in the setup or termination of associations
- All invalid messages (invalid signature, sequence number out of order, Generalized Time out of scope, sender not authorized for the implied request)
- All incoming messages that may cause changes to the NPAC SMS database

7.9.3.7 Key Exchange

R7-107.1 Lists of Keys

NPAC SMS shall ensure that during a security key exchange, each party provide the other with a list of keys.

R7-107.2 Keys in Electronic Form

NPAC SMS shall provide the list of keys in a secure electronic form.

R7-107.3 Paper copy of MD5 Hashes of the Keys

The originator of the list of keys shall also provide the receiver with signed (in ink) paper copy of the MD5 hashes of the keys in the list.

R7-107.4 Key List Exchange

NPAC SMS shall support exchange of the list of keys in person or remotely.

R7-107.5 Remote Key List Exchange

NPAC SMS shall convey the lists via two different channels, diskette sent via certified mail, and a file sent via Email or FTP using encryption mechanisms if the keys are exchanged remotely.

R7-108.1 Remote Reception Acknowledgment

NPAC SMS shall support the Service Providers' acknowledgment via 2 secure electronic forms, Email or FTP using encryption mechanisms.

R7-108.2 Acknowledgment Contents

NPAC SMS shall support the acknowledgment consisting of the MD5 hash of each one of the keys in the list.

R7-108.3 Phone Confirmation

The recipient shall call the sender by phone for further confirmation and provide the sender with the MD5 hash of the whole list.

R7-109.1 Periodic Paper List of Public Keys NPAC Uses

NPAC SMS shall generate a paper list to each Service Provider of the MD5 hashes of all the public keys used by a Service Provider once a month.

R7-109.2 Acknowledgment of Paper List of Public Keys

NPAC SMS shall verify the identity of the Service Provider to whom the MD5 hashes of the public keys was sent.

R7-110.1 List Encryption Keys

NPAC SMS shall provide each Service Provider with a numbered list of encryption keys, numbered from 1 to 1000.

R7-110.2

(Duplicate - refer to R7-107.2)

R7-110.3 List Encryption Keys

NPAC SMS shall ensure unique numbering of the keys.

R7-111.1 New Encryption Key Can Be Chosen

NPAC SMS shall allow a new encryption key to be chosen with every message that contains a key identifier.

R7-111.2 Keys Not Reused

NPAC SMS shall reject messages that use a key whose usage has stopped.

R7-111.3 Compromised Keys

NPAC SMS shall allow authorized NPAC SMS personnel to initiate a new key for messages.

R7-111.4 Key Change Once Per Year

NPAC SMS shall change the key used between the NPAC SMS and Service Provider after one year of usage.

R7-111.5 Key Size Increase Per Year

NPAC SMS shall allow NPAC SMS personnel to change key sizes for Service Providers as needed to ensure secure communications between the NPAC SMS and the Service Providers.

R7-111.6 Per Service Provider Application Basis

NPAC SMS shall expect new key initiation to be requested on a per Service Provider application basis.

RR7-1 Load Key List

NPAC SMS shall be able to load a new key list in 15 minutes or less.

This change order should be sized as a point release as early as possible during or prior to turn-up testing with the service providers.

RN7-1 Authenticator Contents - Individual System Clock Accuracy

NPAC SMS shall be responsible for ensuring that the system clock is accurate to within two minutes of GMT.

RN7-2 Authenticator Contents - Zero Sequence Number

A sequence number equal to zero shall be required for association request and association response messages.

RR7-2 Modifying User Name

NPAC SMS shall provide a mechanism for authorized NPAC personnel to change a user name in the NPAC SMS.