International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1125

(01/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Correlative Reacting System in mobile data communication

Recommendation ITU-T X.1125

ITU-T

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1125

Correlative Reacting System in mobile data communication

Summary

In a mobile network environment, while core networks are able to manage security threats, mobile stations (MSs) that access the mobile network have little defence capability due to limited hardware resources. Compromised mobile stations can themselves easily become virus agents and threaten the entire network. The Correlative Reacting System (CRS) defined in this Recommendation aims to protect mobile networks against the threats of insecure terminals that do not conform to the security policy of the network, such as terminals that have been compromised.

Source

Recommendation ITU-T X.1125 was approved on 13 January 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Page

Recommendation ITU-T X.1125

Correlative Reacting System in mobile data communication

1 Scope

Focusing on end-to-end data communication in mobile networks, this Recommendation describes the open architecture of the Correlative Reacting System (CRS), which protects the network against potential security threats from insecure mobile terminals. This architecture provides operator networks with enhanced security capability through mobile station (MS) security updates, network access control and application service restrictions. This results in a mechanism that prevents viruses or worms from spreading rapidly through the network operator.

This Recommendation provides an abstract level architecture and is an application of current implementation-level protocols in the wired/PC world, e.g., trusted network connection (TNC) specifications for the mobile network scenario. Where appropriate, existing proven concepts and elements from the wired world should be reused as much as possible in the design and implementation of CRSs.

This Recommendation specifies Correlative Reacting System application protocol (CRSAP) messages which can be transferred using XML or compact binary encodings as specified in Annex A.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.680] Recommendation ITU-T X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.691] Recommendation ITU-T X.691 (2002) | ISO/IEC 8825-2:2002, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.

[ITU-T X.693] Recommendation ITU-T X.693 (2001) | ISO/IEC 8825-4:2002, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*.

[ITU-T X.694] Recommendation ITU-T X.694 (2004) | ISO/IEC 8825-5:2004, *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*. <http://www.ietf.org/rfc/rfc2748.txt>

[W3C XSD] W3C XML Schema (2004), *XML Schema Part 0: Primer Second Edition*. <http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 application service [ITU-T X.1121]: A service like mobile banking, mobile commerce, and so on.

3.1.3 application server [ITU-T X.1121]: An entity that connects to an open network for data communication with mobile terminals.

3.1.4 application service provider (ASP) [ITU-T X.1121]: An entity (person or group) which provides application service(s) to mobile users through an application server.

3.1.5 availability [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.6 data integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.7 data origin authentication [ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.8 denial of service [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.9 privacy [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

NOTE – Because this term relates to the rights of individuals, it cannot be very precise and its use should be avoided except as motivation for requiring security.

3.1.10 mobile network [ITU-T X.1121]: A network that provides wireless network access points to mobile terminals.

3.1.11 mobile security gateway [ITU-T X.1121]: An entity which relays data communication between a mobile terminal and an application server, changes security parameters or communication protocol from a mobile network to an open network, or vice versa, and can perform security policy management functions for mobile end-to-end data communication.

3.1.12 mobile terminal [ITU-T X.1121]: An entity that has wireless network access function and connects a mobile network for data communication with application servers or other mobile terminals.

3.1.13 mobile user [ITU-T X.1121]: An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers.

3.1.14 system security function [ITU-T X.803]: A capability of a system to perform security-related processing, such as encipherment/decipherment, digital signature, or the generation or processing of a security token or certificate conveyed in an authentication exchange.

3.1.15 security communication function [ITU-T X.803]: A function supporting the transfer of security-related information between open systems.

3.1.16 security transformation [ITU-T X.803]: A set of functions (system security functions and security communication functions) which, in combination, operate upon user data items to protect those data items in a particular way during communication or storage.

3.1.17 threat [ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application service controller (ASC): A mobile network element that performs application service access control on mobile subscribers. By correlatively reacting with the security correlation server (SCS), it imposes service restrictions on specified unsafe users based on the application service control policy of CRS.

3.2.2 controlled object: The mobile station (MS) controlled by the CRS. A controlled object may be a single MS or a group of MSs.

3.2.3 Correlative Reacting System (CRS): A mechanism that enables mobile terminals or devices and the network to cooperate together against potential security threats, such as viruses, worms, Trojan-horses, user misbehaviour and other network attacks.

3.2.4 Correlative Reacting System application protocol (CRSAP): An application layer protocol for CRS message encapsulation and transport between the SCA and the SCS.

3.2.5 dedicated security device (DSD): A device that provides dedicated security functions for the network (e.g., firewalls, IDs, security gateways, and security management servers).

3.2.6 mobile station (MS): Any mobile device, such as a mobile handset or computer, which is used to access network services.

3.2.7 mobile station operating system (MSOS): Functionality that can automatically perform self-update, patch installation or SAS updating in cooperation with the MSOS-US and the SAS-US according to SCS instructions received by the SCA.

3.2.8 mobile station operating system updating server (MSOS-US): A server that provides service patches, software updates, and upgrades for the MSOS.

3.2.9 network access controller (NAC): A mobile network element that provides control of user access to the network. It has the capability to perform data-bandwidth-access limitation upon a specified unsafe user, according to network access control policies. The network access device is normally a network gateway, e.g., SGSN in the mobile network.

3.2.10 policy: A collection of rules applied in CRS to enforce the proper control on MSs.

3.2.11 security application software (SAS): Software that provides a specific class of security function for a terminal or device within the network system. For example, anti-virus software.

3.2.12 security application software updating server (SAS-US): A server which is located on the network side to provide security files or profile updating and other online security services to terminals or devices.

3.2.13 security correlation agent (SCA): A module embedded in mobile terminals to collect the security-related environmental information, to communicate with the security correlation server (SCS) in the mobile network for security evaluation, and to provide the terminal or device with updated security information.

3.2.14 security correlation information (SCI): Information correlated with the security environment for mobile terminals or devices, such as the version control of the operating system and anti-virus software used in the mobile terminal or device.

3.2.15 security correlation server (SCS): A server in a mobile network that communicates with the security correlation agent (SCA) for evaluating the security degree and environment of mobile terminals or devices.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and accounting
API	Application Programming Interface
ASC	Application Service Controller
ASP	Application Service Provider
CN	Core Network
COPS	Common Open Policy Service
COS	Chip Operating System
CRS	Correlative Reacting System
CRSAP	Correlative Reacting System Application Protocol
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSD	Dedicated Security Device
GGSN	Gateway General Packet Radio System Support Node
GPRS	General Packet Radio System
H-ASC	Home Application Service Control
H-NAC	Home Network Access Control
H-SCS	Home Security Correlation Server
HLR	Home Location Register
Ic	CRS communication Interface between SCA and SCS
Ica	Communication interface between SCA and other SAS
Ics	CRS communication interface between SCS and NAC/ASC
IP	Internet Protocol
IPSec	Internet Protocol Security
L1	Layer one, i.e., physical layer

L2	Layer two, i.e., data link layer
MS	Mobile Station
MSOS	Mobile Station Operating System
MSOS-US	Mobile Station Operating System Updating Server
NAC	Network Access Controller
OS	Operating System
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
P-TMSI	Packet TMSI
QoS	Quality of Service
RAN	Radio Access Network
RBAC	Role-Based Access Control
SAS	Security Application Software
SAS-S	Security Application Software Server
SAS-US	Security Application Software Updating Server
SCA	Security Correlation Agent
SCI	Security Correlation Information
SCS	Security Correlation Server
SDB	Security Data Base
SGSN	Serving General Packet Radio System Support Node
SIM	Subscriber Identity Module
SOC	Security Operation Centre
SUS	Security Updating Server
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMSI	Temporary Mobile Station Identity
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
V-ASC	Visited Application Server Control
V-NAC	Visited Network Access Control
V-SCS	Visited Security Correlation Server
WLAN	Wireless Local Area Network
XSD	eXtensible Markup Language Schema Definition
WiMAX	Worldwide Interoperability for Microwave Access

WTLS	Wireless Transport Layer Security
XML	eXtensible Markup Language

5 Conventions

None.

6 Overview of the Correlative Reacting System

Along with the popularization of wireless data networks, an increasing number of people use mobile terminals to enjoy new network services. Packet data services will eventually replace the traditional circuit-switched services; meanwhile, mobile telecommunication networks tend to be unified IP-based networks. The traditional specifications for security mechanisms proposed by 3GPP, WLAN and WiMAX ensure the security of user access, authentication and message transmission. However, application layer threats (e.g., viruses, worms, hacker attack, and hijacking user information) are still emerging endlessly, which result from the openness of mobile network architecture and the inherent security vulnerabilities of IP technology. Since every node/host/user is equal, there exists a risk that one compromised node can threaten the whole network. Unfortunately, the security mechanisms referred to in this Recommendation cannot deal with these problems.

It is easy to manage the security threats from inside operator core networks, but it is difficult to do this from mobile stations that have access from the core network or via the access network. Due to the limited resource, mobile stations (MSs) have little defence ability. Hence, if the operating system (OS) or security application software (SAS), e.g., host firewall is not updated in a timely manner, the MS will be more vulnerable to a successful virus attack. Furthermore, if an MS with significant mobility becomes virus-infected, it could itself become a virus vector and endanger the network operator. Therefore, it is very difficult for the operator to make an appropriate compromise between network security guarantees and high services-quality guarantees for the users.

In the field of classical wired networks, the specifications of trusted network connect (TNC) architecture processed by Trusted Computing Group (TCG) provide terminal integrity for a host (e.g., a personal computer) that accesses a network, i.e., only those who are authenticated on the network side and conform to network security policy are allowed access to the network. However, there is little consideration of the problems that are specific to a mobile network, such as mobility, roaming, hardware capability of terminals, and unreliability of the link via air interface, etc. Referring to the end-to-end security features of mobile data services described in [ITU-T X.1121], the proper service features of the mobile network user will require further consideration. For example, after an MS is infected by some viruses or worms, it may send junk messages or attack messages to the data network, which can result in unreasonable charges, or sharply reduce the capability of the mobile network or cause other problems. In addition, there can be other issues, such as the split between SIM card and mobile terminal, as well as the independent wireless access protocol. These issues will also require further consideration.

Due to the rapid development of wireless applications and the increasing number of the third party ASPs, business tends to focus on value-added services and sophisticated management. As a result, there is an increasing number of threats against MSs and mobile networks, while mobile subscribers are using diverse services. For example, a corporation may disclose the interior resources to unauthorized users, such as the identity of an employee who accesses the Intranet via wireless network. Furthermore, there is the potential for application systems to be abused or to be destroyed, resulting in a reduction in application quality or unavailability of the application.

Because of rapid development, virus technology can generate mass traffic in a network when a virus breaks out in large scale. The mass traffic resulting from junk data or attack traffic flow will have a severe negative impact on the efficiency and the security of the operator's network and will also negatively impact the security and the application of mobile users.

The Correlative Reacting System (CRS) aims to protect mobile networks against the threats of insecure terminals that do not conform to the network security policy, such as the terminals that are virus-infected or that have been otherwise compromised. Meanwhile, CRS also aims to prevent the MSs from becoming infected through periodical evaluation and updating of the MS's security configuration and through assisting those virus-infected MSs to recover.

Attacks can be divided into two categories: network-layer-based network attacks and application-layer-based service attacks. The former take place during the course of establishing a wireless network connection and before the network provides the application service; the latter happen after the wireless connection is established and during the period of service. Such division of attacks into two main categories is to emphasize that CRS can provide different types of access control services: access to the network bearer resources; and access to the network service resources via NAC and ASC, respectively. Similar to the PC/wired world, the main purpose of CRS is to counter the network attacks limited to connection establishment. However, through periodical SCI reports (see clause 8.2.3, SCI report policy) and evaluation of the terminal security status, CRS can support the capability for the network operator to counter other attacks such as those during communication (and even some system attacks) by virtue of the collected user terminal security information.

To resist the threats resulting from insecure terminals, CRS provides multi-layer access controls: network access control (NAC) and application service control (ASC) to ensure that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications (see [ITU-T X.805]). These two types of control complement each other. In one instance, NAC supplements the limitations of ASC and effectively controls the risk from the complex mechanisms such as network worms and hacker attacks. In the other instance, ASC makes it possible to limit the impact on network traffic that is caused by an attack against some specific network service(s) as well as to prevent the spread of any infection.

Aiming at the mobile end-to-end application data service, the CRS establishes an infrastructure to protect against the threats described as follows:

– for the mobile subscriber, compromise of private information of the subscriber; and abuse of subscriber toll services;

– for the terminal system, protects against the mobile station becoming a denial of service (DoS) attack agent when the MS system is defective or unavailable;

– for the mobile network system, protects against the spread of viruses or worms that cause network congestion and waste network resources (i.e., QoS reduction); and

– for the application service system, loss of availability of application and server services due to service layer attacks or virus infection in the server or the MS; unauthorized disclosure of subscriber information; and integrity impairment.

The essence of CRS is to control network access and to restrict access to the application services of mobile stations by correlatively reacting between mobile stations and the network, so that the CRS can provide the network with the capability to counter network threats such as viruses and other network attacks.

The global AAA architecture defined in [b-IETF RFC 2903], [b-IETF RFC 2904], [b-IETF RFC 2905] and [b-IETF RFC 2906] has some relationship with CRS in that they share common user information. The CRS procedures should be combined with AAA-related authentication and authorization procedures, usually after the AAA user authentication and before authorization to the terminal to access the network resources. However, such issues should be considered in the implementation phase of CRS and this is currently out of the scope of this Recommendation.

7 CRS description

7.1 Preconditions

The implementation and the performance of CRS services rely on the correlative reacting cooperation with a number of other external functions as described below:

- the network can enforce network access control for the network based on the network layer;
- the network can enforce control on application service access for the network based on the application layer;
- the security application software updating servers (SAS-USs) and mobile station operating system updating servers (MSOS-USs) can provide automatic and timely security updating services for user terminals[1];
- dedicated security devices (DSD) deployed on the network side can provide specialized security functions for the network. Examples of DSDs include firewalls, security gateways, security operation centres (SOCs) and intrusion detection and prevention systems;
- the security application software (SAS) can provide the security correlation agent (SCA) with particular security information about the terminal, and can automatically perform security updating in cooperation with an SAS-US according to CRS instructions; and
- The mobile station operating system (MSOS) can provide the terminal's security-related system configuration information, and can automatically perform security updating in cooperation with the MSOS-US according to CRS instructions.

The entities that can achieve these external functions are able to communicate with CRS entities (e.g., SCA and the security correlation server (SCS)) via the interfaces defined in this Recommendation and it is assumed that the entities, in cooperation with CRS, can enforce CRS security policies via the interfaces.

In addition, the transmission of a CRS message is based on current transport layer protocols, e.g., TCP and UDP; while, the security of the CRS message is protected by security protocols, e.g., TLS (see [b-IETF RFC 4261]), IPSec (see [b-IETF RFC 4301]), and WTLS (see [b-OMA WTLS]).

7.2 CRS objectives

The following objectives are used to guide the design of CRS:

- by using real-time security evaluation of the terminal side of the air interface and real-time control on the MS, the CRS has the ability to limit the spread of network threats, and thus assure the security of the network;
- the network side of the air interface assists MSs in related security updating;
- the CRS has the ability to ensure that mobile data service and CRS message transmission can keep running as normal while the MS moves between CRS-enabled network and a network that does not have CRS enabled;
- the CRS has the ability to guarantee the availability of the SCA. Specifically, the CRS must detect the SCA configuration when an MS connects to the network. If the MS is not SCA-enabled, the SCA should be installed and enabled. If the MS is SCA-enabled, the CRS must keep the SCA up to date; and

[1] Unless otherwise noted, the term *security updating* in this Recommendation means software updating and upgrading, which includes program updating, program upgrading, patch installation, and so on.

– one SCS may simultaneously control a single or multiple NAC/ASCs. Each NAC/ASC has a default SCS to connect, but one NAC/ASC must simultaneously connect to multiple SCSs. This will allow security policy to be enforced without interruption even if the default SCS encounters problems.

7.3 CRS system architecture

The aim of the Correlative Reacting System is to solve the potential security threats against mobile networks that are caused by insecure mobile stations. Based on the security evaluation of the MS, the CRS can direct network equipment to process network access control and application control on the MS, and to assist the MS in related security updating. The CRS provides both the mobile network and the MS with some specific security enhancements. Furthermore, CRS provides a mechanism to limit the spread of network security threats, such as viruses and worms.

Figure 1 illustrates the CRS architecture and environment.

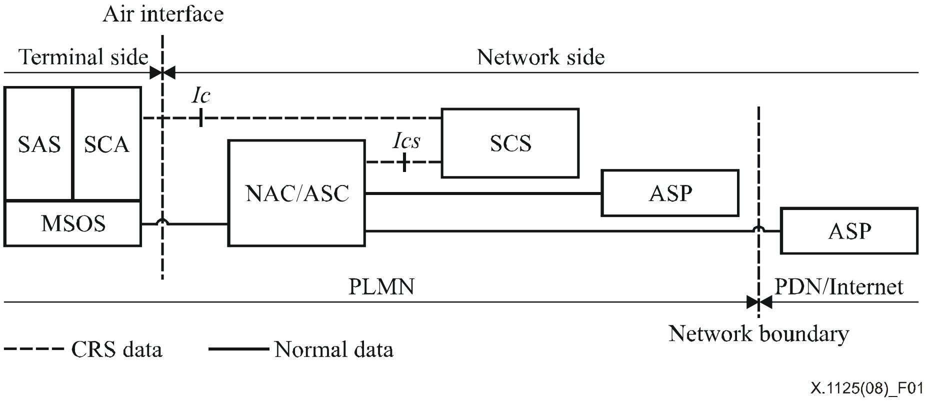


Figure 1 – CRS architecture and its environment

A CRS system comprises four entities:

– a security correlation agent (SCA). The SCA is installed on the MS;

– a security correlation server (SCS). The SCS processes the control on the NAC/ASC and SCA;

– a network access controller (NAC). The NAC executes the control on the MS network access; and

– an application service controller (ASC). The ASC executes the control on the MS application service access.

The SCA lies in the terminal side, while the SCS, NAC, and ASC are located in the network side.

The SCA communicates with the SCS via the interface *Ic* (see clause 7.5.1), and the SCS communicates with other network elements via the interface *Ics*. By their communication and interaction, the CRS provides the function of security-focused control on mobile stations.

The SCA is responsible for collecting security-related environmental information and communicating it to the SCS. This collection is essential for the SCS to evaluate the terminal's security level and to further determine what network services can be accessed.

After receiving the SCA security report on the mobile terminal, the SCS carries out the evaluation for the MS. If it decides that the terminal is not secure enough, the SCS will notify the SCA and request the NAC or ASC to enforce the specified user control policy (see clause 8.2.2). In addition, if the SCS decides that the terminal needs upgrading, a process that relies on the SAS-US or MSOS-US, the SCS will instruct the SCA to initiate the necessary upgrading immediately.

If there are applicable security updates, such as OS patches, component updates or security-related patches for the application software, the SCS must direct the SCA to assist the MS in processing related upgrading or updating. All update programs are stored in the SAS-US and the MSOS-US, which also provides a security updating service.

The updating of the SCA is also closely associated with the MS's security. When the SCS detects that the SCA's software is not the latest applicable version, it will instantly inform the SCA and instruct the SCA to upgrade or update the software.

As shown in Figure 1, application service providers (ASPs) may deploy their own services in a mobile network, while the operator of the mobile network can also be considered as an ASP. These ASPs should configure their *Ics* interface, via which they can communicate with the SCS and acquire some information (such as a list of insecure mobile stations). In this way, it is possible for the ASP server to enforce application access control.

Network access or application service access control on mobile users is achieved through the SCS's control on the user's mobile station. Related security information is primarily acquired from the SCI report sent from the SCA to the SCS. For those SCA-enabled mobile stations, the SCA will be initiated as soon as the MS connects to the data network.

Practical network entities functioning with the CRS include, but are not limited to, the following dedicated security devices (DSD):

– firewalls (provide security protection for network boundary);

– security gateways (terminate connections and operate as proxies);

– security management servers (provide knowledge of network side and the support of policy for the SCS); and

– intrusion detection and prevention systems, anomaly detection systems (analyse network traffic, detect network intrusion or attack, and filter its virus traffic or attack traffic).

7.4 CRS entities

7.4.1 Security correlation agent (SCA)

7.4.1.1 Functions of a security correlation agent

Figure 2 shows the functional structure of a security correlation agent.

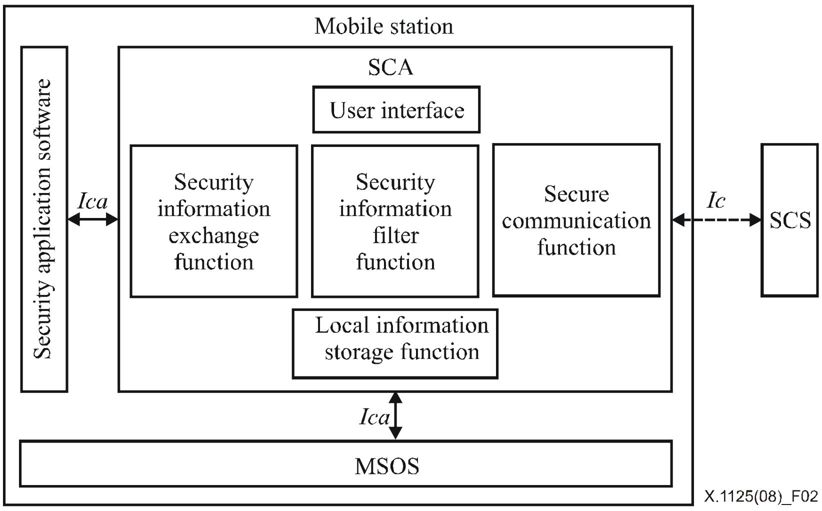

Mobile station
SCA
User interface
Security application software
Ica
Security information exchange function
Security information filter function
Secure communication function
Ic
SCS
Local information storage function
Ica
MSOS
X.1125(08)_F02

Figure 2 – SCA functions

The SCA has five primary functions as described below:

1) *Exchange security-related information*

   The SCA collects security-related information from the MS. This information includes: MS security events; the OS version and patch; the version of the SAS; SAS log information; the mobile user's ID; and the MS's ID, etc. Based on security upgrading information and information received from the SCS, the SCA provides the MS's OS and security application software with security updates or upgrading information via the interface *Ica*. In the real world, security application software has its own update/upgrade channel. *Ica* is a logical interface which can be used to bear such a SAS-specific message exchange channel.

2) *Analyse and filter information*

   According to local policy or policy received from the SCS, the SCA is able to process and organize the MS security-related information, which will be filtered and reported to the SCS. Meanwhile, the SCA also has the ability to receive the information from the SCS, which includes security status and upgrading information, the result of the security evaluation of the MS, and access control information, etc. After filtering, the information must be reported to the mobile user or must generate a local security report/log, that can be queried by the user.

3) *Secure communication*

   This function is responsible for the security transformation, the mutual authentication with the SCS, and to negotiate and establish the secure communication tunnel with the SCS, and thus ensure that the transmission of the CRS message between the SCA and the SCS is reliable.

4) *User interface*

   This function enables information to be exchanged between the user and the SCA, providing the user with security-related information and enabling the user to query security-related information, including the SCI report, and the security evaluation result, etc. The SCA has the capability to generate a MS security status report for each user query based on the collected MS security-related information and the SCS. Generally, the security status report is stored as an SCA running log. If the SCS decides that the MS has a lower security level or if severe security events happen on the MS, the SCA can notify the user in order to alert the user to possible threats.

5) *Local data storage*

   This function stores SCA-related security information, logs and various policies.

7.4.1.2 Requirements for the security correlation agent (SCA)

The SCA has the capability to:

- collect security-related information from the mobile station;
- report MS security-related information to the security correlation server (SCS);
- automatically discover the existence of the SCS;
- respond to SCS messages;
- report related information to the user when necessary;
- assist mobile terminals in updating OS and security-related software;
- guarantee the authenticity of data from the *Ica* interface;
- guarantee the confidentiality and integrity of locally-stored information; and
- forbid the user to modify the configuration of the SCA.

  NOTE – The configuration can be dynamically modified only by the SCS according to the evaluation of the security conditions of both the MS and the network.

7.4.2 The security correlation server (SCS)

7.4.2.1 Functions

The security correlation server (SCS) is a logical entity comprising several functional modules as follows, each of which can be physical equipment. The SCS functional architecture is described in Figure 3.

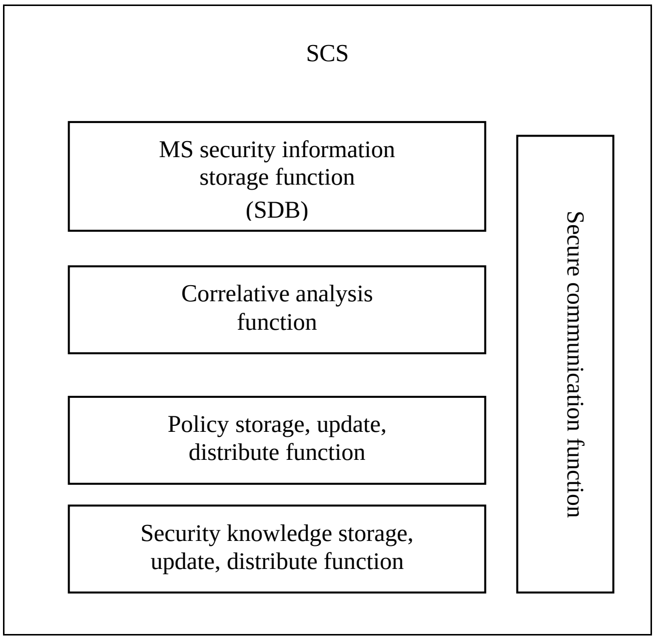

SCS
MS security information storage function (SDB)
Correlative analysis function
Policy storage, update, distribute function
Security knowledge storage, update, distribute function
Secure communication function

Figure 3 – SCS functions

The SCS has five primary functions as described below:

1) *Communication function*

This function is responsible for establishing a reliable and secure tunnel between the SCS and the SCA, as well as between the SCS and NAC/ASC. It guarantees the integrity and the confidentiality of the CRS messages. It also enables the information exchange among different SCS functional modules.

2) *Storage function of MS security-related information*

The SCS comprises one security database (SDB). This database is used to store SCI reports sent by the SCA, the security evaluation result of the MS and the current active control policy for MSs. There may be one particular sub-database to describe the current and historical relationship among mobile user identities, mobile terminals, and SCA IDs.

3) *Correlative analysis*

According to the stored security policy and security knowledge, the SCS utilizes SCI reports to evaluate the security level of a single MS. Furthermore, the SCS may determine the security condition of certain areas of a mobile data network by correlatively analysing SCI reports sent from multiple MSs and the security evaluation result of a single MS.

4) *Storing, updating and delivering policy*

The policy comprises policy for system control and policy for security evaluation (see clause 8.1). The policy should be defined and stored in the SCS. Utilizing the SCS communication function, the SCS can deliver the policy to the SCA, NAC and ASC. These policies are then used to guide their behaviours. An interface for policy management should be provided to help either administrators or the exterior policy management unit to update the stored policy, either manually or automatically.

5) *Storing, updating, and delivering security knowledge*

Security knowledge comprises all security knowledge and information provided by the network side of the air interface. It includes:

i) diverse and known network security threats and their solutions;

ii) patches, information about the upgrading package and the URL of the resource for MSOS;

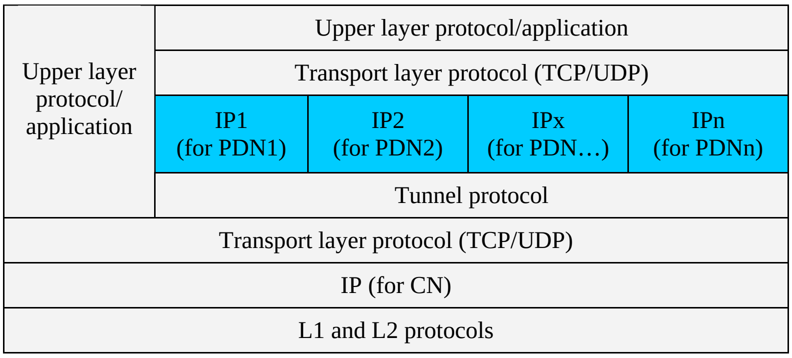
iii) patches, information about the upgrading package and the URL of the resource for MS security-related software; and

iv) SCA version information and the URL for download.

For the CRS, it is very important to keep security knowledge updated. Security knowledge affects how fast the CRS can react to known security threats. OS producers, SAS producers and third party security research institutions should provide most of security knowledge for the CRS.

Security knowledge is used to guide the MS process security-related updating. Meanwhile, it acts as reference information that is utilized for SCS correlative analysis and for constituting security policy.

An example of the SCS protocol stack structure is illustrated in Figure 4. The SCS has a static IP address in the core network (CN). This IP address is used by the SCS for communication within the core network area. Moreover, the SCS has another kind of IP address. Above the layer of tunnel protocol, the SCS has some other static IP addresses (IP1 for PDN1, IP2 for PDN2, …, IPn for PDNn). Each IP address is associated with one PDN which is directly connected to the mobile network or core network. These IP addresses are used by the SCS to communicate with mobile stations or with network elements accessing or belonging to the associated PDN. The packets of this kind of communication are encapsulated as tunnel protocol (IP-in-IP encapsulation) packets within the core network area and are unencapsulated into normal IP packets outside the core network area.



<table>
<tr><td rowspan="4">Upper layer protocol/ application</td><td colspan="4">Upper layer protocol/application</td></tr>
<tr><td colspan="4">Transport layer protocol (TCP/UDP)</td></tr>
<tr><td>IP1
(for PDN1)</td><td>IP2
(for PDN2)</td><td>IPx
(for PDN…)</td><td>IPn
(for PDNn)</td></tr>
<tr><td colspan="4">Tunnel protocol</td></tr>
<tr><td colspan="5">Transport layer protocol (TCP/UDP)</td></tr>
<tr><td colspan="5">IP (for CN)</td></tr>
<tr><td colspan="5">L1 and L2 protocols</td></tr>
</table>

Figure 4 – SCS's protocol stack structure

7.4.2.2 Requirements for the security correlation server

The SCS has the capability to:

– acquire security-related information of the MS;

– acquire security policy and security knowledge on the network side;

- determine the MS security level based on analysing and evaluating the MS security status;
- assist insecure mobile stations in security-related updating;
- control the SCA's behaviours and to update SCA when necessary;
- establish a secure communication tunnel with the SCA and to acquire the MS security-related capability information;
- establish a secure communication tunnel with the NAC/ASC; and
- obtain security statistics about MSs connected to one data network or one domain.

7.4.3 Network access controller and application service controller

The network access controller (NAC) and the application service controller (ASC) control mobile stations accessing the mobile data network (e.g., SGSN in [b-3GPP GPRS]). Both the NAC and the ASC are logical concepts. The difference between them is in their respective control functions. The NAC primarily aims to control the establishment, maintenance and release of the connection of MSs with the network after MS authentication, while the primary responsibility of the ASC is to restrict MS access to particular application services.

The NAC/ASC communicates with the SCS via the *Ics* interface. The involved content can be divided into two categories:

1) *The NAC/ASC sends the SCS related information about the MS*

   The related information about the MS refers to information that is demanded by the SCS and that can be acquired from the NAC and the ASC (e.g., in 3GPP, the mobile user ID, MS PDP context, MS capability information, etc.).

2) *Receive and enforce the control policy delivered by the SCS*

   The NAC/ASC receives and enforces user control policy that is generated and delivered by the SCS, and then feeds back the enforcement result.

As the equipment is on the network side of the air interface, the NAC/ASC can acquire diverse capability information about the MS while the MS is attaching to the mobile data network. When the MS connects to the network, the NAC/ASC should instantly send SCS-related information (e.g., MS capability information, PDP context and mobile user ID in [b-3GPP GPRS]) in order to inform the SCS that the mobile user has started using the packet data network. At this point, the CRS starts dynamic control on the MS.

7.5 CRS interfaces

7.5.1 *Ic* interface

The *Ic* interface enables the communication between the SCA and the SCS. The SCA sends SCI reports to the SCS, based on which SCS returns response messages. The response messages carry SCA control policy (see clause 8.2.3) and/or security update information.

Before exchanging MS security-related information between the SCA and the SCS, secure communication must be guaranteed. For example, WTLS (see [b-OMA WTLS]) or IPSec (see [b-IETF RFC 4301]) are candidate protocols for the security mechanisms to establish a security tunnel. See clause 9 for details of communication and request of the *Ic* interface.

7.5.2 *Ics* interface

The *Ics* interface is utilized in the communication of control policy-related information between the NAC/ASC and the SCS. The NAC/ASC requests the control policy for a controlled object (i.e., a single MS or MS group) from the SCS. After determining the security level of the controlled object, the SCS returns the appropriate policy.

The *Ics* takes the existing transport layer protocol (e.g., TCP) to ensure the communication is reliable. How the NAC/ASC and the SCS entities are addressed can be statically configured in related entities. After the NAC/ASC acquires the SCS address, a communication tunnel between them will be established. Furthermore, for the security of the communications between the SCS and the NAC/ASC, some security mechanisms, e.g., TLS (see [b-IETF RFC 4261]) or IPSec (see [b-IETF RFC 4301]) must be applied.

8 CRS policy

8.1 Security evaluation policy

8.1.1 General

The primary function of the CRS is to evaluate and determine the security level for every single MS. Specifically, based on the security evaluation policy, the SCS analyses the security conditions of every single MS (i.e., MS SCI report) and then determines the security level of the MS. The CRS adopts a security control policy for the MS according to the security level of the MS. The idea of protecting users and the network with a security level disperses the policies involved in CRS and makes it more adaptive and more specific for diverse situations. This enables rationalization of policy enforcement.

The material policy for security evaluation is not defined in this Recommendation. However, the basic principle is provided in this clause.

This clause may be used to guide the selection of policy language relating to the implementation of a CRS system. The existed security/vulnerability assessment data formats and vulnerabilities and vulnerability disclosure languages, e.g., [b-OASIS AVDL] and [b-OSVDB] may be reused if they meet the requirements described in this clause.

8.1.2 Parameters of security evaluation

Various parameters are the basis for the CRS to evaluate and determine the MS security level. These parameters are mainly obtained from the security information within the terminals via the local *Ica* interface. Normally, the CRS needs security information of at least two terminals to analyse it synthetically.

The *Ica* interface enables information exchange between the SCA and the MSOS/SAS. Via the *Ica* interface, the SCA can acquire security-related information from the MSOS and the SAS. In addition, the SCA transfers appropriate information to the MSOS and the SAS for security updates of the terminal. As the SCA is an application-layer functional entity, the *Ica* interface can be implemented based on the API of the MSOS. Through the API of MSOS, SAS applications can also communicate with the SCA via the local *Ica* interface. The information received by the SCA should be trustable and unforged, and the information should not be disclosed to other unauthorized entities. In addition, integrity protection should be provided during the transfer process.

The security information contains security configuration information and/or security event information. The former includes system security-configuration information and application security-configuration information. Security event information includes virus event information, attack event information, and the results of illegal information scanning, etc. Specifically, four kinds of parameter, as shown below, can be extracted from the security information.

Table 1 – Parameters of security evaluation

User information parameters	User identity	User identity is used to associate the user with a corresponding security level and control policy decision.
	Subscribed services	This parameter is used for evaluating whether the MS security problems will bring risk when using the services. This factor influences CRS to evaluate the MS security level. It can be obtained from the network side.
	Current service	This parameter is used for evaluating whether the MS security problems will bring risks to the current user service. This is an important factor for CRS to determine whether it is necessary to interrupt the current user service. The information of this parameter can be obtained from the network side.
MSOS/platform information parameters	OS/platform type	Different operating systems have different security problems. Generally, the greater the market share, the more threats that will be faced.
	Version number	In general, older versions of operating systems have more hidden troubles.
	Situation of installed patch	Patch for OS/platform is very important for the system security. It may indirectly lead the system to be attacked by popular viruses if some key patches have not been installed.
	Situation of current open ports	For security reasons, it is recommended for OS/platform to close unnecessary communication ports because opening more ports would create more hidden security problems.
SAS information parameter	SAS type	This parameter indicates what security software the MS has installed and what functions the SAS can provide. Normally, the more types of SAS that have been installed and the more powerful the security software functions are, the more secure the system is. However, they consume more local resources of the MS.
	Version number	Generally, newer versions of SAS have more powerful security safeguards.
	Result of virus and Trojan detection	This important parameter affects the evaluation of MS security level. In general, the MS will be set at a high security level if some devastating or highly infective virus or Trojan is detected and cannot be cleared or killed.
	Result of attack detection	This parameter indicates the situation of the MS being attacked.
	Security log	This parameter is the result of the security situation from the analysis by SAS. It can be an important reference of the security evaluation.
	Version of virus definition file	The virus definition file shall be kept updated. The newer version means more security threats can be detected and further avoided.
	Version of SAS URL information	This parameter can be used to evaluate whether the URL information in the SAS has the latest version or not.
Terminal information parameter	Type of mobile terminal	This parameter provides the type and the version of the terminal. Different types of terminals have different security characteristics. For instance, a laptop that accesses a mobile network may have more threats to the network than a cell phone. Besides, it will affect the security evaluation when security leaks are found in terminal products.

8.1.3 Classification of security level

The MS security level can be basically divided into two classes: MS aggressive security level and MS vulnerability security level, both of which roughly have three ranks: high, medium and low.

- Aggressive security level indicates the extent to which a mobile station poses a threat to other users or to the network. Based on the aggressive security level of the MS, the CRS places restrictions on MS activities to differing extents.
- Vulnerability security level indicates the degree of vulnerability of the mobile station to attack. The CRS instructs the MS to reinforce its security status (e.g., security updating) to an extent consistent with the vulnerability level of the MS.

Aggressiveness and vulnerability are not completely independent of each other. In fact, there is some relationship between them and they may co-exist or transform sometimes. For example, a vulnerable terminal may become a virus infector after being infected by virus, and hence it becomes aggressive. Generally, for comprehensive security evaluation, one MS has both kinds of security level simultaneously.

Classification of aggressiveness and vulnerability levels is indicated below:

- High aggressiveness: an MS can threaten other users and the network directly and seriously. The threat, if realized, is devastating and highly infective, and has a strong possibility of being carried out, e.g., virulent virus.
- Medium aggressiveness: an MS can threaten other users and the network to a limited degree. The threat, if realized, is devastating and infective and has a moderate possibility of being carried out, e.g., DoS attack based on MSs.
- Low aggressiveness: MS has little potentiality to threaten other users and the network. The threat has low probability of being carried out, e.g., adware.
- High vulnerability: the MS is highly vulnerable to attack at any time; the users will be seriously affected, e.g., serious leaks of sensitive information about the operational system.
- Medium vulnerability: the MS is somewhat vulnerable to attack or the MS may be affected to a limited extent, e.g., too many ports are open in the operational system.
- Low vulnerability: there is little potential for the MS to be attacked or the MS may be affected to a small degree, e.g., both OS and security software are up to date.

The method to determine security levels for MSs depends on the practical condition of the network and the numerous factors listed in Table 1; therefore, it is difficult to define an overall level. To make CRS useful in deployment, the security level should also be decomposed according to practical factors, such as the integrity, availability and confidentiality requirements of each service.

8.1.4 Principles of constituting policy

Considering the security guarantee and QoS guarantee of the core network, the control policy should make a moderate compromise between the security and the QoS depending on different security levels. There are two basic principles that constitute policy based on the security level:

1) Precedence principle: the precedence principle means to determine which aspect (QoS or security) should be guaranteed first according to security levels. When precedence is given to QoS, there will be a delay in enforcing the security policy. Conversely, if security is given precedence, security policy will be enforced and the service may be immediately interrupted.

2) Mandatory/optional principle: the mandatory/optional principle is used to determine the basis for implementing policy. If optional, the decision can be made by the user; if mandatory, the system enforces policy implementation.

Several reference principles of security policy creation are as shown below:

– High aggressiveness: security is given preference and it is mandatory to implement the security policy. The user's current service can be interrupted or limited when necessary.

– Medium aggressiveness: the service is given preference and it is mandatory to implement the security policy. The user's service can be limited when necessary.

– Low aggressiveness: the service is given preference and it is optional to implement the security policy. The user can decide to accept or reject the security policy. There is no limit in user service.

– High vulnerability: security is given preference and it is mandatory to implement the security policy. The user's current service can be interrupted or limited if necessary.

– Medium vulnerability: the service is given preference and it is mandatory to implement the security policy. The user's service can be limited if necessary.

– Low vulnerability: the service is given preference and it is optional to implement the security policy. The user can decide to accept or reject the security policy. There is no limit in user service.

8.2 Security control policy

8.2.1 General

Security control policy is defined and stored in the SDB of the SCS. These control policies correspond to the security level, and the relationship between them is configured by the SCS. From a functional perspective, the policy can be divided into two categories: user control policy and SCA control policy. The former is used by the SCS to direct network access equipment (i.e., NAC or ASC) to control or restrict users trying to access network and/or application services. The latter is utilized to control the SCA and to collect and report MS security-related information in a timely manner. Because the control policy should be defined by operators themselves, this clause provides only principles for achieving it.

8.2.2 User control policy

User control means that the SCS, by the correlative reaction of the SCS and the SCA, utilizes some technical methods (such as flow control, access restriction or QoS reconfiguration), to restrict a user's network access. This can reduce the risk of insecure terminals unreasonably utilizing a network resource as well as limiting the spread of viruses.

For access restriction, the policy is designed to be broadly configurable. It could be set as no restriction, full restriction or partial restriction. No restriction means that no control actions will be taken on terminals. Full restriction means that the terminal cannot access any network resources. Partial restriction means that the terminal is allowed (or forbidden) to access some specific addresses. These specific addresses can be divided into two types: trusted address and restricted address. The former refers to the address of secure terminals or ASPs. Generally, MSOS-US and SAS-US are involved in this type. The latter refers to the address of those terminals or ASPs that are insecure.

For redirection, access to the network is permitted, but all the message flow should be redirected to some dedicated security devices (DSD), such as an anti-virus firewall. DSD will filter messages first, and if it finds that a message might lead to spreading of a virus, it discards the message; otherwise, the message is forwarded to the destination address.

For QoS reconfiguration, the CRS will adjust the quality of service for terminals according to the MS security status. Generally, the improvement of the MS security status leads to the enhancement of QoS.

The reference principle for policy design, relying on the MS security level, is provided in Table 2.

Table 2 – User control policy

MS security level	User control policy
High aggressiveness	Full access restriction or Redirection
Medium aggressiveness	Redirection QoS reconfiguration (e.g., bandwidth limited) Only access to trusted addresses is permitted
Low aggressiveness	No restriction
High vulnerability	QoS reconfiguration (e.g., bandwidth limited) Only access to trusted addresses is permitted
Medium vulnerability	Only access to restricted addresses is forbidden
Low vulnerability	No restriction

In addition, when the SCS does not receive the SCI report sent by the SCA, based on SCA control policy, the SCS is not able to evaluate the current MS security status. Meanwhile, to protect network security, the NAC enforces default network access control policy. The default NAC policy may be to forbid a user's access to any network resource. Alternatively, it may also be to redirect all messages sent from the MS to the DSD, which will then forward the messages to the destination.

8.2.3 SCA control policy

The SCA control policy comprises the SCI report policy and the SCI collection policy.

SCI report policy

The SCI report policy specifies when an SCA should send an SCI report to the SCS and what content should be included in the SCI report. The SCS determines the period for sending the SCI report and specifies what security events can trigger the SCA to send the SCI report instantly (e.g., the MS is virus-infected, the MS has been attacked by a hacker, or a user has uninstalled some SASs). Depending on the time sent, the SCI report policy can be divided into four categories.

1) *Initial SCI report policy*

   When the MS connects to a data network and the SCA receives a SCA probe request, the SCA must send to the SCS an initial MS SCI report. The report provides the SCS with comprehensive knowledge of the MS security conditions. As a result, the SCS can evaluate the MS security conditions as comprehensively as possible and the SCS can then determine the MS security level. The initial SCI report should include all security evaluation parameters mentioned in clause 8.1.2.

2) *Periodic SCI report policy*

   After the MS connects to the data network, the SCA should periodically send a SCI report to the SCS until the MS disconnects from the data network. The initial setting of the periodic SCI report is the SCA default report period and default report content. Basic information involved in the periodic SCI report includes the changes of the MS security conditions and statistical information of security events (e.g., attack type, attack times and attack originator) during the report period.

   During the connection, the SCS can instantly adjust the SCI report period and report content according to changes in network security conditions or the MS security level. For example, if the MS security level changes from a low aggressive level to a high aggressive level, the SCS may instruct the SCA to shorten the report period and/or to increase report content for stronger monitoring of MS security conditions. This allows the CRS to take timely corresponding control actions for the MS when necessary. Conversely, it can also be applied to prolong the report period and/or to lessen report content.

In accordance with the MS security level, the reference principle of periodic SCI report policy design is shown in Table 3.

Table 3 – Periodic SCI report policy

MS security level	Periodic SCI report policy
High aggressiveness	Frequently sent SCI report Comprehensive reported information
Medium aggressiveness	Default SCI report period Default reported information
Low aggressiveness	Shorten report period Lessen reported information
High vulnerability	Frequently sent SCI report Report comprehensive information
Medium vulnerability	Default SCI report period Default reported information
Low vulnerability	Shorten report period Lessen reported information

3) *Security events SCI report policy*

Any security events occurring on the MS will trigger the SCA to send an SCI report in order to inform the SCS. Regardless of whether the security event results in the loss or destruction of MS data, it should be reported to the SCS instantly. For example, if an MS was infected by a virus that was quarantined or cleaned, even if it did not cause any damage to MS security, the SCA still needs to report the event to the SCS. Based on these security events reports, the SCS may correlatively analyse all security events that have happened in the network to predict the network threat trend, which helps the CRS to actively protect network security and MS security.

The security event report should cover the following information:

a) The type of security event (such as virus infections, network attacks, un-installation or modification of SAS, communication ports opened/closed, application services enabled/disabled).

b) The name of the security event

c) When the event happened

d) The originator of the security event

e) What actions have been taken by SAS

f) Other related information

For instance, to report a virus that infects a MS, the security event report should include virus type, virus name, infected time, originator of the virus, the type of infected files, and what actions have been taken by the MS anti-virus software.

4) *Requested SCI report policy*

When the SCS temporarily needs the SCA to report security-related information of the MS, it can initiate a request for an instant SCI report from the SCA. The SCA must report the requested information to the SCS at the time specified by the SCS.

SCI collection policy

The collection of security correlative information is implemented via the *Ica* interface. The collected information should cover the following items:

- Information related to the MSOS
- Information related to the SAS
- Information related to the mobile terminal equipment

All information is collected by related software, and then it is transferred to the SCA via the *Ica* interface. The detailed description of the collected information is provided in clause 8.1. The time when the SCA collects information directly depends on the SCI report policy. As a result, this is out of scope of this Recommendation.

8.3 Group attribute management

To improve the efficiency of the CRS, the CRS can support group management. For every online MS, the SCS can dynamically configure its group attribute based on its evaluation result. Furthermore, the configuration of the group attribute should be kept consistent among the SCS, NAC/ASC and SCA.

After an MS connects into the network, the SCS can analyse and evaluate the related status information of the MS. The SCS then configures the group attribute for it. An MS can join multiple groups at the same time, i.e., one can have a multi-group attribute. In addition, according to different purposes and different deployments of the CRS, group attributes can be classified diversely, e.g., MS-type group, location group, security-level group and service-type group, etc. Table 4 gives an instance of group attribute application.

Table 4 – Group attribute of one MS

Type of group	Group ID	Description
MS-type group	Type-PDA	PDA mobile stations
OS-type group	OS-Windows mobile	The OS of MSs is Windows mobile
Location group	LA-A	MSs located at location area A
Security-level group	SecLevel-V3	MSs with high vulnerability evaluated by SCS
Service-type group	Service-VIP	MSs with subscribed VIP level security service

To facilitate the success of group management of the CRS, the SCS should make the NAC and the SCA aware of the MS's group attribute. To achieve this, the SCS can inform the NAC of the MS's group attribute by the first control policy indication sent to the NAC; or the SCS can inform the SCA by the first SCI response. During the period of connection, the SCS can still update the MS's group attribute by a control policy update message or SCI response.

A group attribute can be applied in all kinds of CRS procedures, including updating the user control policy for MSs, sending an updating instruction to multiple MSs, initiating a request SCI report from multiple MSs, and so on. Clause 12.1 describes a specific application of group attribute management.

NOTE – Modern policy languages, e.g., role-based access control (RBAC), could be used where appropriate when managing the above-mentioned group attributes in the implementation of CRS.

9 Communication between SCA and SCS

9.1 Message carrier protocol

The CRS application protocol (CRSAP) is utilized to achieve message transmission between the SCA and the SCS. There are some messages, such as those for entity discovery (see clause 11.1) that use acknowledgement mode, i.e., sender's messages need to be acknowledged by the receiver. While most messages carrying security-related information (e.g., SCI reports) may use either acknowledgement mode or un-acknowledgement mode (see also clause 11).

The CRSAP layer is located over the transport layer. The CRSAP may work on either a reliable transport layer protocol (e.g., TCP) or an unreliable transport layer protocol (e.g., UDP). The choice of transport layer protocol depends on the security requirements of the message type and its content.

9.2 Security

All messages exchanged between the SCA and SCS are application layer messages. The secure communication tunnel used may be based on TLS, WTLS and IPSec, etc. The CRS does not restrict the choice of security mechanism. In addition, almost all CRS messages transmitted between the SCA and the SCS should use a secure communication tunnel except for special cases, e.g., where the network initiates large-scale security updating for MSs.

If there is no immediately-available secure communication tunnel and the CRS messages are required to be transmitted securely, the SCA should first request the establishment of the secure tunnel from the SCS.

9.3 Messages

9.3.1 General

The CRSAP uses both XML schema definition (XSD) and a compatible ASN.1 specification to define its message format and content. Either specification (see Annex A) can be used to determine an XML encoding of CRSAP messages. The ASN.1 specification can be used to determine a compact binary encoding of CRSAP messages. One CRSAP message is normally comprised of three parts:

– message header;

– message body; and

– message tail (optional).

An example of an XML schema definition and the equivalent ASN.1 specification are included in Annex A, and an SCI report is provided in Appendix II.

9.3.2 Message header

The CRSAP message header is a summary of the message and its length should be fixed. It should include the following elements:

– 'Version'

  This is the version number of the CRSAP protocol. The version field is defined as '1.0' now.

– 'Flag'

  This is a string and it indicates whether the CRSAP message is a multicast or unicast message and if the message contains a message tail or not.

Table 5 – Flag in message header

Flag	Flag description
M	Multicast message without message tail
MT	Multicast message with message tail
U	Unicast message without message tail
UT	Unicast message with message tail

– 'Precedence'

This is used for the message receiver to decide the processing precedence of the message. It is marked by the message sender.

– 'Type'

This is a string used to identify the direction and the type of the transferred message between the SCA and the SCS. Recommended message types are listed in Table 6.

Table 6 – Message type

Message type	Message	Transform direction	Message tail included?
U_SCI_Rpt	SCI report	Upstream	Recommended
U_SCA_Prb_Rsp	SCA probe response	Upstream	Optional
U_Ack	Acknowledgement	Upstream	Optional
U_Err_Ntf	Error notification	Upstream	Optional
D_SCI_Rsp	SCI response	Downstream	Recommended
D_Prb_Req	SCA probe request	Downstream	Optional
D_Rep_Req	SCI report request	Downstream	Required
D_Ack	Acknowledgement	Downstream	Optional
D_Err_Ntf	Error notification	Downstream	Optional

– 'Length'

This indicates the total length of the message header, message body and message tail.

– 'SCS-ID'

This is the globally unique identifier of the SCS.

– 'SCA-ID'

This is the identifier of the message related to the SCA(s), which is unique in the SCS controlled area. It is dynamically assigned by the SCS. In addition, SCA-ID may be an identifier of a group of multiple SCA entities.

9.3.3 Message body

The size of CRSAP message body is flexible. Table 7 lists some primary information elements for each message type. However, it should be mentioned that not all the listed elements for each message would be involved per time.

Table 7 – Information elements in message body

Message type	Information element	Description
SCI report	Rpt_ID	The serial number of SCI report
	MS_Usr_ID	Identity of MS user
	MT_ID	Device identity of mobile terminal
	MS_OSPlt_TypVer	MSOS/platform type and version
	MS_OSPlt_PatLst	MSOS/platform patches information
	MS_SAS_Inf	MS SAS type, version, database
	MS_Sec_Evt	MS security event information
	MS_Hrd_Inf	MS hardware information
	SCI_Cur_RptPol	Reporting current SCI report policy to SCS
	SCS_LstCom_Inf	Domain, address, port and SCS ID of the SCS communicated last time
SCI response	MS_Sec_Lev	Evaluation result of security level
	SCI_New_RptPol	New SCI report policy to SCA
	SCS_Lmt_Ntf	Notice about limit of user network access and/or application service
	Ack_SCI_Rpt	Acknowledgement of SCI report
SCA probe request	SCS_Domain	The domain of the SCS
	SCS_Address	The address of the SCS
	SCS_Port	CRS service port of the SCS
SCA probe response	Lst_SCS_Domain	The domain of the last attached SCS
	Lst_SCS_Address	The address of the last attached SCS
	Lst_SCS_ID	SCS ID of the last attached SCS
	Lst_SCA_ID	SCA ID used in the last CRS communication
SCI report request	Lst_SubMsg	List of requested SCI
	Tim_ Rpt	The requested report time
Acknowledgement	MsgID_Ack	The message ID of acknowledged message

9.3.4 Message tail

The message tail is an optional item in the CRSAP messages. It can be used for the message receiver to check the integrity and to process data origin authentication. When the applied security protocol (e.g., IETF TLS, IPSec) provides the function, CRSAP messages may omit the message tail. Otherwise, the message tail must be included in all CRSAP messages. One message tail includes three parts:

– 'AlgorithmID': Algorithm ID identifies the related crypto algorithms for message integrity and origin check.

– 'MsgID': Message ID is the serial number of CRSAP messages. The count of message ID should be different for different transfer directions.

– 'MsgDigest': Message digest is the hash value of CRSAP message header and message body.

10 Communication between the NAC/ASC and the SCS

10.1 General

In the CRS, communication between the NAC/ASC and the SCS aims to ensure effective delivery and enforcement of user control policy, i.e., effective control over the MS user based on policy.

[RFC 2748] is recommended to be used in carrying the messages transferred between the SCS and the NAC/ASC. The SCS acts as a policy decision point; the NAC/ASC acts as a policy enforcement point. The NAC/ASC requests control policy from the SCS. The SCS returns the control policy decision. If the SCS determines that it is necessary to update user control policy, it will deliver an updated policy decision to the NAC/ASC on its own initiative.

Similar to the messages specified in COPS, the messages between the SCS and the NAC/ASC are described in detail in the following clauses.

10.2 Message security

The security of all CRS messages is assured or provided by carrier protocol. Message-level integrity must be assured, although COPS considers it as optional. In addition, transport layer security must be provided by using TLS or IPsec.

10.3 Messages

10.3.1 Control policy request

For every controlled object, the NAC/ASC sends an object policy request message to request the user control policy for objects controlled by the SCS.

The content of this message should involve the following information elements:

– Request number

  This is assigned by the NAC/ASC. It uniquely identifies one control policy request. One controlled object uniquely corresponds to one request number.

– Requested policy type

  The policy can be used for network access control or application service control.

– Type of controlled object

  The controlled object can be a single MS or an MS group.

– Identifier of controlled object

  For a single MS, the mobile user ID together with mobile equipment ID may be applied; for an MS group with the same security level, the security level code may be applied.

– Controlled object related information

  Additional information, such as MS addressing, may be needed. For example, if applied in a GPRS network, for a single MS, the information should include the MS PDN address, the routing area identity and security-related information.

There are two occasions for the NAC/ASC to request user control policy from the SCS:

1) *NAC/ASC requests SCS for policy*

When the MS acquires the PDN address after it connects into the network, the NAC/ASC should send a message to report the connection of the MS and to request the user control policy for the MS. After receiving the report, the SCS should instruct the NAC to enforce the default user control policy, which should enable the MS to access the SCS. Then, the SCS should try to locate the SCA and communicate with the SCA to acquire the MS initial SCI report (see clause 11.1). Optionally, the SCS can utilize the acquired mobile user identity to query the MS customized service and the historical index of the SCI report stored in the SCS.

2) *The SCS instructs the NAC/ASC to initiate a request for policy*

The SCS instructs the NAC/ASC to send a new control policy request to acquire a new control policy decision for a group of MSs with the same security level or within the same area. The new control policy decision is generated by the SCS based on statistical information of the MSs' security level and location.

10.3.2 Control policy delivery

When the SCS receives the object policy request message, it determines what user control policy is adapted to the controlled object and then delivers the policy decision to the NAC/ASC, which enforces the control on the controlled object according to its received policies.

If the SCS does not know the current security conditions of the controlled object after receiving an object policy request message, i.e., the SCS does not receive the MS SCI report, the SCS instructs the NAC to control user network access based on default policy. The default control policy may be to prevent the user from accessing any network resource. Alternatively, it may also be to redirect all messages sent from the MS to the DSD, which will then forward the messages to the destination.

Hereafter, an external event (e.g., the SCS receives an SCI report and the network administrator directly modifies the policy stored on SCS) can trigger the SCS to update the user control policy by sending a subsequent object policy decision to the NAC/ASC. The subsequent object policy decision indicates to the NAC/ASC what policy should be deleted and/or installed.

If the SCS does not receive a periodic SCI report at the specified time or if the SCS does not receive a requested SCI report, the SCS considers the security conditions of the MS as opaque. It then instructs the NAC/ASC to enforce the default user control policy and initiate the SCA discovery procedure (see clause 11.1) and, in addition, the SCA auto-installation procedure (see clause 11.3).

In addition, when the SCS decides it is necessary to deliver the user control policy for a new controlled object, the SCS can instruct the NAC/ASC to send a new object policy request so that the SCS can deliver the policy to the NAC/ASC. For instance, based on the statistical result of all SCI reports from diverse MSs, the SCS can decide to deliver a unique user control policy for one MS group.

Whenever the NAC/ASC receives an object policy decision, a policy enforcement response message must be returned to inform the SCS of the result of enforcing the policy. If the policy enforcement has failed, the NAC/ASC enforces the last available user control policy while the NAC/ASC sends a SCS policy decision response carrying the information about what policy was used and why the policy has failed to be enforced.

10.3.3 Policy enforcement status report

During the connection, the NAC/ASC must periodically report current SCS control status with respect to the object controlled. The report must include the list of current enforcing policies and statistical information about enforcement of each policy. By doing this, it is possible for the SCS to know the efficiency of each control policy.

10.3.4 Control policy synchronization

By analysing the received policy enforcement status report and the SCI report, the SCS can detect whether the user control policy being enforced by the NAC/ASC is identical to the SCS's policy decision or not. If the answer is negative, the SCS instructs the NAC/ASC to execute a control policy synchronization procedure, which is described below:

1) the SCS instructs the NAC/ASC to execute the control policy synchronization procedure;

2) after receiving the instruction, the NAC/ASC resends an object policy request for the controlled object;

3) the SCS returns the comprehensive policy decision for the controlled object;

4) the NAC/ASC receives the policy and informs the SCS of the implementation of the control policy synchronization.

10.3.5 Control policy termination

When the NAC/ASC detects that there is no need to execute control on some controlled object (e.g., the MS leaves the network or is out of the control area), the NAC/ASC should inform the SCS of the termination of control policy provision.

11 General procedures in CRS

11.1 The discovery of SCA/SCS

For those SCA-installed MSs, the SCA needs to know the SCS address so that the SCA can communicate with the SCS. Here, the address refers to the PDN address of the SCS, e.g., the IPv4 address or the IPv6 address. Figure 5 illustrates one method for the CRS to locate the SCS.

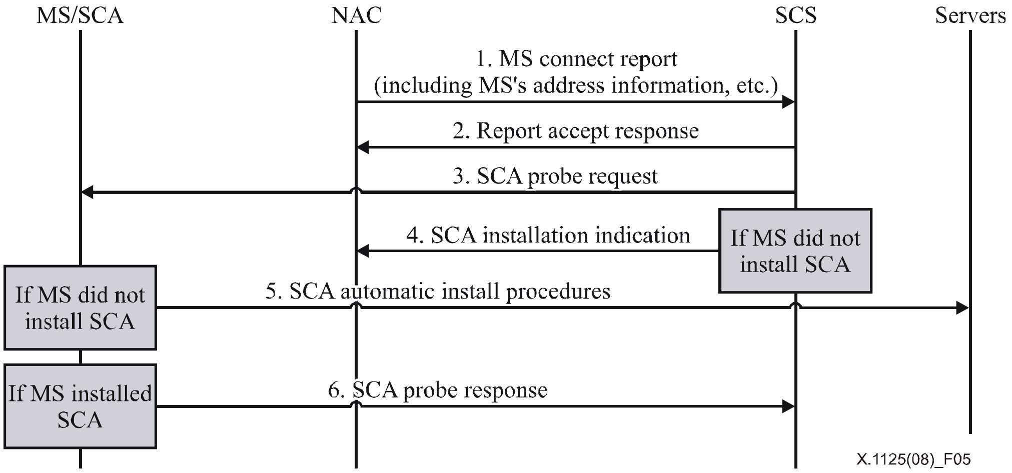

MS/SCA
NAC
SCS
Servers
1. MS connect report
(including MS's address information, etc.)
2. Report accept response
3. SCA probe request
4. SCA installation indication
If MS did not install SCA
If MS did not install SCA
5. SCA automatic install procedures
If MS installed SCA
6. SCA probe response
X.1125(08)_F05

Figure 5 – The discovery of SCA/SCS

1) After the MS connects to the mobile data network by normal authenticating, charging and acquiring an IP address, the NAC instantly sends an MS connect report to the SCS to inform the SCS of the new MS connected to the CRS-employed data network. The MS connect report includes information about the MS address, the location, the mobile user ID, the mobile station ID, and the MS capability.

2) The SCS acknowledges the receipt of a valid MS connect report.

3) The SCS sends the MS SCA probe request to detect whether the MS is SCA-enabled and whether the SCA is operating normally. The SCA probe request includes the SCS address and service port information, which is used by the SCA to do necessary configuration initialization of the communication with the SCS. It may be necessary for the MS to roam into other data networks that employ CRS and this mechanism is adaptive when MS roams into a data network that does not employ CRS as well. If there is no SCS in a network that does not employ CRS, the MS cannot receive an SCA probe request message at all. As a result, the SCA can determine that there is no CRS in the MS connected network.

4) If the MS does not respond to the SCA probe request message correctly within a specified time, the SCS considers that the MS does not have SCA installed or the SCA on the MS does not work normally. In this case the SCS informs the NAC that the MS needs SCA installation, followed by step 5.

5) If the MS does not have SCA enabled, the SCA auto-installation begins. This part is described as a single procedure in clause 11.3.

6) If the SCA on the MS works normally, after receiving an SCA probe request from the SCS, the SCA will instantly respond to the SCA probe request. If the SCS receives the SCA probe response, it considers that the SCA on the MS works normally, thus the MS does not need SCA installation.

11.2 SCI report and MS control procedure

In CRS, the MS security-related information report sent from the SCA to the SCS is called the security correlation information (SCI) report. This report is primarily utilized by the SCA to inform the SCS of the MS security status, which assists the SCS in evaluating the MS security level. According to the MS security level, the SCS processes appropriate control on the MS and helps the MS to do the related update. There are thus two aspects to assure the security of the mobile network, i.e., real-time control on the network side and security enhancement on the terminal side.

The SCI report contains the following content:

a) Report serial number

The report serial number is an incremental positive integer, which identifies the sequence of all SCI reports during one data network connection. Utilizing it, the SCS can tell whether the SCI is retransmitted, lost or out of sequence.

b) SCA ID

The SCA ID uniquely identifies one installed SCA on the MS. It identifies the party to whom the SCS should send the SCI response. If the SCA receives one message from the SCS but the SCA ID is not in accordance with its own ID, the SCA considers it an error and drops this message, following which it sends an error notice to the SCS. The SCA ID can be assigned by the SCS of the visiting network. When the MS moves to another CRS domain, the SCA ID might be reassigned.

c) Mobile terminal ID

The mobile terminal ID uniquely identifies one mobile device. For many kinds of mobile phone, the international mobile equipment identity can act as a mobile terminal ID.

d) SCS ID

The SCS ID uniquely identifies one SCS. If the SCS ID involved in one received SCI report is not in accordance with its own ID, the SCS drops this message.

e) Mobile user ID

The mobile user ID uniquely identifies one mobile user. According to it, the SCS determines the user's identity and allows customized services or other differentiated services.

f) The body of the SCI report

The body of the SCI report comprises all MS security-related information sent from the SCA to the SCS. It includes:

i) Type, version, patch and open ports information of the MSOS;

ii) Type, version, database, security event and log information of the MS SAS;

iii) Subscription services, current service information of MS user;

iv) Type, hardware information and device identity information of the MS;

v) Reporting information about detection of viruses, Trojan horses and other attacks;

vi) Domain, address, port and SCS ID of the SCS communicated the last time.

The SCA sending the SCI report and the SCS's control process for MSs is the most basic of the CRS procedures. This procedure happens when the MS finishes authentication and connects to the data network. Hereafter, the SCA installed on the MS is activated and then generates and sends an SCI report to the SCS to start the communication with the SCS. After analysing the SCI, the SCS determines the security level of the MS, then delivers the corresponding control policy to the NAC/ASC, which enforces the control on the MSs. The SCS may pre-deliver some control policy to the NAC/ASC as local or default policy of the NAC/ASC. In this case, it is not necessary for the NAC/ASC to request policy for every incident.

The SCI report and the MS control procedure are depicted in Figure 6.

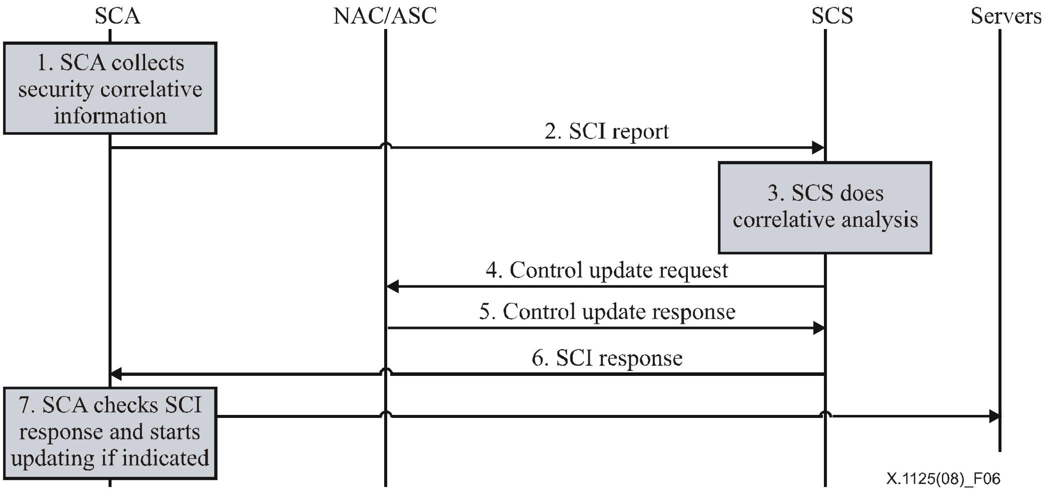

SCA
NAC/ASC
SCS
Servers
1. SCA collects security correlative information
2. SCI report
3. SCS does correlative analysis
4. Control update request
5. Control update response
6. SCI response
7. SCA checks SCI response and starts updating if indicated
X.1125(08)_F06

Figure 6 – SCI report and MS control procedure

1) The SCA collects security-related information of the MS.

2) The SCA generates the SCI report based on the information referenced in step 1. The generation of the SCI report should be based on the SCI report policy (see clause 8.2.3). The SCA sends the SCI report to the SCS.

3) After receiving the SCI report, the SCS initially confirms its validity, and then correlatively analyses it, relying on security evaluation policy, in order to determine the security level of the MS.

4) If the SCS considers that it is necessary to update the NAC/ASC enforcing policy for the MS, one control message carrying the new policy decision (see clause 10) will be sent to the NAC/ASC.

5) If step 4 happens, the NAC/ASC must feedback the enforcement result of the user control policy updating.

6) The SCS sends the SCI response to the SCA in order to inform the SCA of the evaluated MS security level. The SCI response can still include the policy for the SCA to generate and send the SCI report, the policy for the SCA to collect and organize the MS security-related information. If the SCS considers it is necessary for the SCA to update the policy to process the security updating, and the address from which the MS can acquire the security update should be included in the SCI response. After receiving the SCI response, the SCA conducts a validity check and then a message analysis. Finally, it utilizes the information to update the SCA local information and policy.

7) If the SCI response message indicates that the MS requires security updating, the SCA assists the MS in security updating according to the information and the policy involved in the message. The referenced security updating still includes the SCA updating and upgrading.

As described in the above procedures, steps 4, 5, and 7 are not used unless they are considered necessary by the SCS.

11.3 SCA auto-installation and auto-updating

11.3.1 SCA auto-installation

In a CRS-deployed network, the MS must install the SCA in order to operate a normal mobile data service. If the MS is not SCA-enabled, or if the SCA cannot work as normal, the mobile network should not only control the user's Internet application and the service provided by the mobile network but should also assist MSs in installing the SCA automatically. The network component that is responsible for this task is the NAC (for example, in GPRS network the SGSN acts as the NAC.)

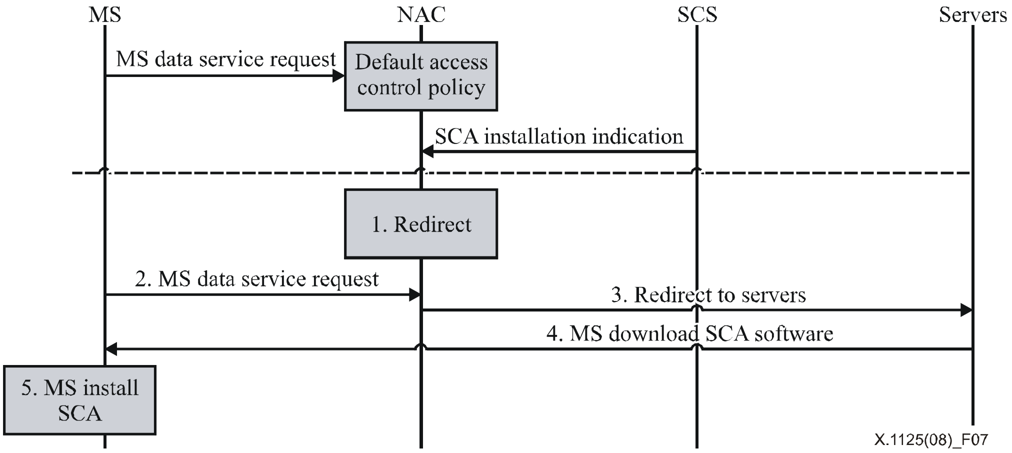

MS
NAC
SCS
Servers
MS data service request
Default access control policy
SCA installation indication
1. Redirect
2. MS data service request
3. Redirect to servers
4. MS download SCA software
5. MS install SCA
X.1125(08)_F07

Figure 7 – SCA auto-installation

The SCA auto-installation in a CRS is shown in Figure 7. It should be mentioned that the following two steps respectively indicate the behaviour of the MS and the NAC before the decision as to whether the SCA needs to be installed is made by the SCS:

1) The MS requests an application service.

2) At this time, the SCS cannot evaluate the security conditions of the MS and the NAC does not know whether the MS needs SCA installation or not. Therefore, the NAC handles messages in step 1 in accordance with the default policy.

The SCA auto-installation procedure begins when the NAC receives the SCA installation indication from the SCS.

1) The NAC receives the SCS's decision that the MS needs SCA installation. The NAC knows that redirection action should be taken on the MS.

2) The MS continues sending messages or requesting an application service.

3) The NAC redirects all service requests of the MS to the server which provides the SCA installation service.

4) The MS communicates with the server to download the adaptive SCA installation program.

5) The MS installs the SCA. After SCA installation, the MS processes the SCA initialization and the SCI report procedure.

Before SCA installation, SCA initialization, and the SCI report procedure, the MS must send persistent messages requesting Internet service. All these messages are forwarded by the IP gateway (i.e., the NAC). By configuration on the network side, the administrator can control the MS's behaviour by controlling these messages. Since the SCS cannot evaluate the security status of the MS at the time, there may be some potential security threats to the whole network in these messages. Therefore, the configuration of the NAC should take these factors into account. For instance, default policy denies the MS access to data network, permits access to only some specific services, or redirects all user-sent messages to the dedicated security device (DSD), such as an anti-virus gateway and firewall.

After the SCA starts working, the SCS acquires the initial SCI report that is generated after the MS connects to data network. After security evaluation, the SCS instructs the NAC to adjust the control on the MS. Afterwards, the MS is able to access the network as normal and security-related updating is applicable when needed.

11.3.2 SCA auto-updating

There are two modes for SCA auto-updating: SCS-initiated and SCI-triggered.

Figure 8 illustrates the procedure of SCS-initiated SCA auto-updating.

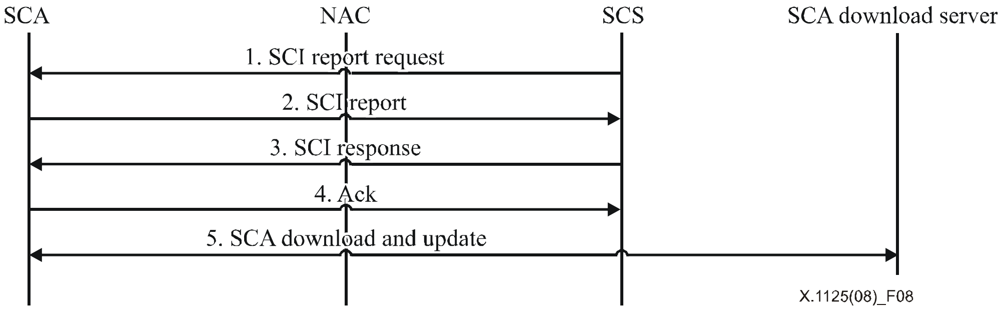


Figure 8 – SCA auto-updating (SCS-initiated mode)

1) When the SCS learns that the SCA has a new release, the SCS sends an SCI report request to the SCA to request the SCA to send an SCI report, which is used to report the release of the SCA on the MS.

2) The SCA reports its release by sending the SCI report to the SCS.

3) After analysing the SCI report, the SCS encapsulates the information related to SCA updating into an SCI response, which is then sent to the SCA.

4) After the SCA acquires updating-related information by analysing the SCI response, the SCA acknowledges the receipt of the SCI response to the SCS.

5) The SCA initiates the SCA updating procedure to download the SCA update program from the SCA updating sever automatically.

If the SCS decides that the SCA needs updating and the SCA sends the SCS an SCI report including SCI release information before the SCS sends the SCA an SCI report request, step 1 (i.e., the SCS sending an SCI report request to the SCA) can be ignored.

As a result, the SCA auto-updating turns into the SCI report-triggered mode. The procedure is illustrated in Figure 9:

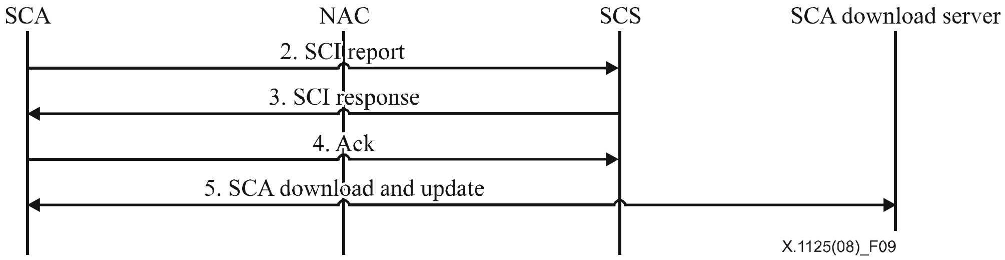


Figure 9 – SCA auto-updating (SCI report-triggered mode)

11.4 Generation and delivery of control policy

When an SCA-installed MS connects to the data network, the SCA should send an SCI report to the SCS based on the SCI report policy. By analysing the information involved in the report and related security information stored in the SCS, the SCS evaluates the MS security level, and then delivers the corresponding user control policy. The detailed procedure is described as follows:

1) The SCS receives a SCI report sent from the SCA.

2) The SCS judges whether the SCI report is in accordance with the SCS-specified SCI report policy:
   i) if the answer is negative, the SCS sends the SCA report rejected message carrying the new SCI report policy;
   ii) if the answer is positive, the SCS filters the SCI report and stores correlative MS security information.

3) Based on the security evaluation policy stored in the SDB and the received SCI report, the SCS evaluates the MS security level and then selects the corresponding user control policy. If the selected policy is different from the enforcing control policy of the NAC/ASC, a security control policy decision message is sent to the NAC/ASC in order to update the enforcing control policy. Meanwhile, the SCS may inform the mobile user of the MS security evaluation result and the enforcing control policy.

4) The SCS correlatively analyses security knowledge and the SCI report. If the result indicates that updating is needed, one SCI response carrying security updating information is sent to the SCA to indicate what update is needed and the address from which the SUS can download the update.

11.5 MS security updating

Similar to SCA security updating, there are two modes for MS security updating: SCS-initiated and SCI-triggered. The detailed procedure of the former is illustrated in Figure 10.

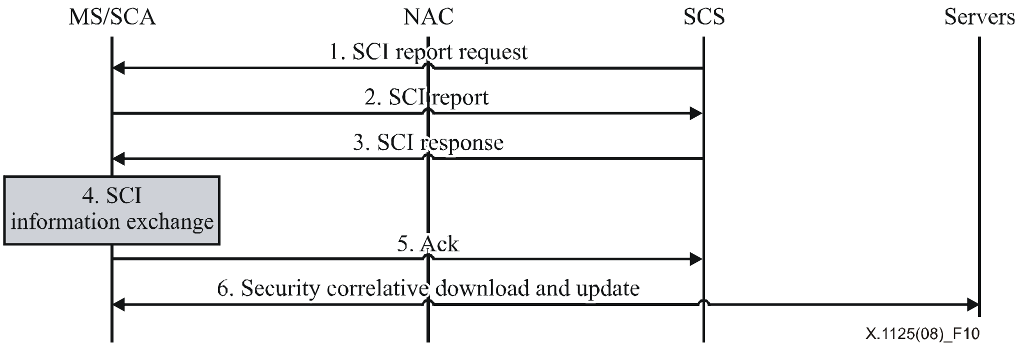


Figure 10 – MS security updating – SCS-initiated mode

1) When the SCS learns that a new update has been released, the SCS sends an SCI report request to the SCA to request the SCA to send an SCI report, which is used to report the MS security-related information including:
   i) The version or the release of MSOS and SAS;
   ii) The information about installed patches (typical examples are the name of the patch and the serial number, e.g., 'patches type_installation object_serial number', and 'OS_Symbian6.0_20061205001');
   iii) The date of database;
   iv) Other relevant information.
2) After organizing and filtering the security-related information collected from the MSOS and the SAS via the *Ica* interface, the MS SCA sends to the SCS an SCI report that encapsulates the related information referred to in step 1.
3) After analysing the SCI report, the SCS encapsulates the MS-adaptive updating information into an SCI response, which will then be sent to the SCA.
4) The SCA analyses the received security updating information contained in the SCI response and then indicates the related updating information to the MSOS and the SAS via the *Ica* interface.
5) If step 4 is successfully completed, the SCA sends an acknowledgement to the SCS.
6) The MSOS and the SAS initiate the updating or the upgrading procedure to receive the security updates from their updating servers.

The referenced servers include the MSOS-US and the SAS-US. In addition, the MS SAS includes firewall, anti-virus software that can be installed on the MS.

In addition, in the above procedure, if the SCS decides that the MS needs security updating and the SCA sends to the SCS an SCI report carrying the security-related information referred to above before the SCS sends the SCA an SCI report request, step 1 can be ignored.

As a result, the MS security updating procedure turns into the SCI-triggered mode. The detailed procedure is shown in Figure 11.

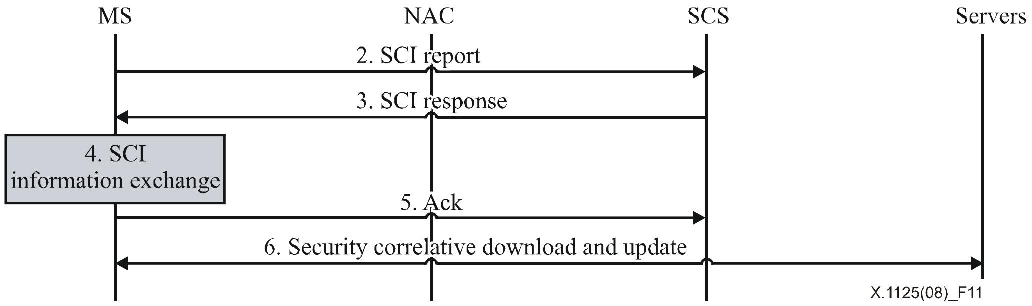

MS
NAC
SCS
Servers
2. SCI report
3. SCI response
4. SCI information exchange
5. Ack
6. Security correlative download and update
X.1125(08)_F11

Figure 11 – MS security updating – SCI-Triggered Mode

11.6 MS leave data network

The procedure for an MS to leave the data network is illustrated in Figure 12.

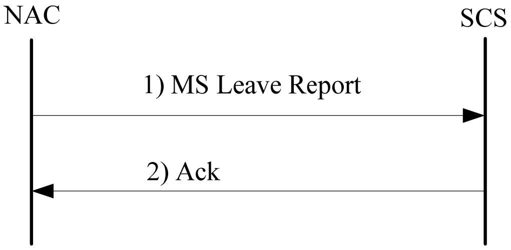


Figure 12 – MS leave data network

1) The MS or network initiates the MS leave data network procedure. After the NAC finishes the MS leave data network procedures that are specified in the related radio network standard, the NAC sends to the SCS an MS leave report informing the SCS that the MS has left the mobile data network. The information involved in the report should include: the mobile user ID, the SCA ID, the mobile terminal ID and the MS address related information.

2) When the SCS receives the MS leave report, it records the status of the involved MS as being offline. Meanwhile, the SCS acknowledges to the NAC the receipt of the MS leave report. The SCS no longer sends any unsolicited messages to the SCA before the MS connects to the data network again.

In the case where the MS abnormally leaves the data network, the mobility management function of the NAC (e.g., the mobility management function of SGSN in a GPRS network) is responsible for the communication with the MS and the maintenance of the connection status between the MS and the mobile data network. In that case, the mobility management function shall first detect this event and then initiate the procedure.

12 Special processing procedures

12.1 Large-scale updating

12.1.1 General

Currently, in the Internet, one robust worm can spread through the whole network very rapidly, without prior warning, resulting in a serious impact on the network. To counter this future threat to mobile networks, large-scale updating is introduced. When the SCS realizes that certain updating is so important that the CRS needs immediate and large-scale security updating to enhance the security status of controlled MSs and to protect the mobile network from attack (i.e., in cases where the security breach addressed would have a serious impact on the security of the network and MSs), the CRS should initiate the large-scale updating procedure.

During the large-scale updating procedure, if too many MSs were to access the SUS and the SCS simultaneously, the procedure would have the effect of a DDoS attack and hence would reduce the availability of the CRS. To avoid this problem, this clause provides a solution based on group management. The whole solution can be executed in three stages: pre-updating, updating and changing to normal updating.

12.1.2 Pre-updating

Before the execution of large-scale updating, the CRS should set the updating-service group attribute for the MS, and then inform the NAC and the SCA of the attribute.

1) Step 1: Setting group attribute

   The setting group attribute is accomplished with an SCI report and the MS control procedure (see clause 11.2) of each MS. As mentioned before, when an initial SCI report is received from one MS, the SCS will evaluate its security status. Based on the evaluation result, the SCS requires the MS to join the relevant updating-service group with relevant precedence during the updating.

   In addition, in compartmentalizing the updating-service group, factors that should be considered include: the types of MS (e.g., laptop, Pocket PC or smart phone), the types of OS/platform (e.g., Symbian, Windows mobile or others), the security level of the MS, objects being updated (e.g., SAS, MSOS or other security-relevant software) and the user-subscribed security service. For instance, those Pocket PCs operated by Windows mobile and evaluated by SCS as high vulnerability level can join updating-service group-A, while those with low vulnerability level can join updating-service group-B. During the large-scale updating procedure, the former will be executed before the latter.

   Based on the consideration of traffic, bandwidth, estimated execution time, and traffic requirements, the number of group members should be limited in order to avoid overloading the network and the CRS.

2) Step 2: Delivery of group attribute

   The delivery of group attribute is also accomplished using the SCI report and the MS control procedure (see clause 11.2) of each MS. When one MS connects to the mobile data network, the SCS should inform the NAC of its group attribute via the first control policy instruction sent to the NAC. Meanwhile, the SCS should do this to the SCA via the first SCI response. During the connection, the SCS can dynamically update the group attribute based on the received SCI report, and can inform the NAC and the SCA of the change by the succeeding control update instruction and the SCI response.

12.1.3 Updating

When the SCS realizes some updating is so important that all relevant MSs must do the updating immediately, the SCS should initiate the large-scale updating procedure. The detailed procedure is illustrated in Figure 13.

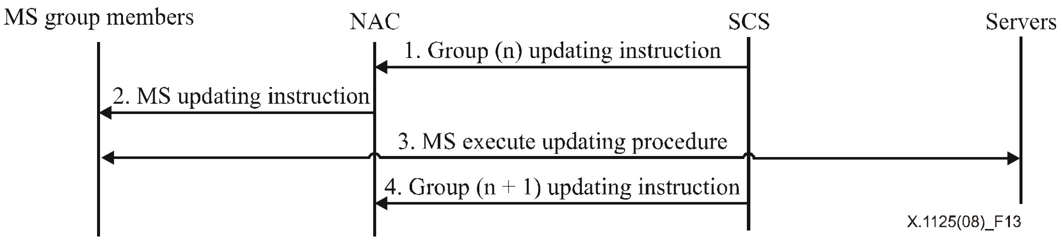

MS group members
NAC
SCS
Servers
1. Group (n) updating instruction
2. MS updating instruction
3. MS execute updating procedure
4. Group (n + 1) updating instruction
X.1125(08)_F13

Figure 13 – Executing group updating

1) SCS sends group (n) updating instruction to the NAC

According to the precedence of the updating-service group, the SCS sends a group updating instruction to the NAC in time order. The information involved in the instruction is shown in Table 8.

Table 8 – Group updating instruction

Item	Description
SCS ID	The identifier of the SCS
NAC ID	The identifier of the NAC
Instruction sequence number	Uniquely identify one instruction
Expiring time	If expired, the NAC should not execute the instruction
Type of instruction	Large-scale updating
Identifier of group	Identify the group to execute updating
Updating resource address	The URL from which MS can acquire the update
MS updating instruction	Encapsulated in the instruction and forwarded by the NAC to all group members
Signature of SCS	The signature for the whole instruction, signed by SCS

2) NAC forwards MS updating instruction to all group members

When the NAC receives the group updating instruction sent by the SCS, it firstly verifies whether the instruction is repetitive or expired. If the answer is negative, the NAC acquires the group ID and updating resource address and also verifies the signature of the SCS. If the verification is successful, the NAC forwards the MS updating instruction to all group members associated with the group ID.

In an emergency, it is recommended that the NAC block all MSs' access to the relevant updating server (except for those MSs currently executing an update) until the NAC receives a succeeding control update instruction from the SCS.

The information involved in MS updating instruction is shown in Table 9.

Table 9 – MS updating instruction

Item	Description
SCS ID	The identifier of the SCS
Instruction sequence number	Uniquely identify one instruction
Expiring time	If expired, the NAC should not execute the instruction
Type of instruction	Group updating
Group ID	Identify the group to execute updating
Object of updating	Indicate what software is to be updated (SAS, OS/platform or SCA)
Type of updating	Patch or Upgrade or Database Updates, etc.
Updating name/code	Uniquely identifies the updating
Updating resource address	The URL from which MS can acquire the update
Signature	The signature for the MS updating instruction, signed by SCS

3) SCA control MS executing the updating procedure

When the SCA receives an MS updating instruction, it first checks whether the instruction is repetitive or has expired. If the answer is negative, the SCA parses relevant updating information and verifies the signature of the SCS. If the verification is successful, the SCA executes the updating.

The SCA then checks whether the specified update is already installed on the MS. If the update is installed, the SCA should instantly send an SCI report to inform the SCS of this status. Conversely, if the update is not installed, the SCA indicates the relevant update object to initiate the updating procedure instantly. Then, the MS accesses the updating resource address in order to download and install the specified update. After installation, the security status of the MS is changed; hence the SCA should then inform the SCS of the change via a security event report.

4) Initiate the updating procedure for the next group

Based on the received SCI report, the SCS can monitor the condition of group updating. If the number of online MSs exceeds the threshold pre-defined by the network operator, the SCS instructs the NAC to do the group updating for next group, i.e., go to step 1.

It should be mentioned that if there are some new MSs connected to the network, the SCS should not directly send updating instruction encapsulated in an SCI response to these MSs or directly make these MSs join the updating-service Group that is executing group updating. The recommended treatment is to make them join the next matched group waiting to execute the updating.

In addition, if there are a number of MSs that connect with the network after the initiation of the last updating-service group and before the last group member finishes its updating, the SCS can add these MSs into a new group as a pending updating-service group.

In an emergency, after all members of one group finish the updating, the SCS should send a control update instruction to the NAC to forbid the members of the group continuous access to the SUS. Then the availability of the succeeding updating service is guaranteed.

12.1.4 Relationship with normal updating

The large-scale updating procedure and the MS security updating procedure are both mandatory parts of CRS. The large-scale updating procedure could be more efficient but is not as flexible as the MS security updating procedure, so it is mostly used in case of emergency or when the network side has just released new important updates.

When the SCS realizes, based on the received SCI report, that group members of updating-service groups have finished updating, the large-scale updating procedure is accomplished. Thereafter, for those MSs that have missed the large-scale updating procedure (e.g., those that connect to the network after completion of the large-scale updating procedure, or those who fail to finish the updating due to some abnormities), the updating procedure should be handled by the MS security updating procedure (see clause 11.5).

12.1.5 Security consideration

In order to guarantee the security of the large-scale updating procedure, the message of the MS updating instruction should include the digital signature of the SCS. After the NAC and MSs receive the MS updating instruction message, they should do the following verification:

1) Verify if the message is really signed by the SCS.

   If it is not, the receiver should discard this message.

2) Verify if the same message has already been received.

   If the receiver has already received and executed the same MS updating instruction which is included in the message, the receiver should discard this message.

Only after the above two verification steps are completed should the MS updating instruction be accepted.

Before each MS begins to update, some informative messages should be sent to MS users to advise them of the need to update and to warn them of the risk if the updating is not done. The MS users have the right to decide whether to accept the update.

13 Handling CRS roaming

13.1 CRS roaming definition

CRS roaming in this Recommendation refers to the case when the MS leaves the coverage area of its controlling NAC/ASC.

13.2 CRS roaming within one CRS-deployed network

The switch of MS control between two NACs or two ASCs within one CRS-deployed wireless data network enables the SCS to communicate with the new NAC/ASC that is responsible for controlling mobile stations, e.g., to deliver control policy to them, to inform the old NAC/ASC to release or terminate the control on the MS.

While the MS switches between the old NAC/ASC and new NAC/ASC (e.g., SGSN in a GPRS network), the routing configuration update (e.g., routing area update in 3GPP GPRS) needs to be processed by the cooperation among network devices, e.g., the MS, the HLR, the new NAC/ASC, the old NAC/ASC, etc. While the MS switches between NACs/ASCs within the CRS-deployed wireless data network, CRS procedures are initiated after the new-NAC/ASC receives packet data service information of the MS (e.g., PDP context in 3GPP), which happens in the MS routing configuration update procedure. The steps for the CRS to process the MS's intra-roaming within the wireless data network are shown in Figure 14.

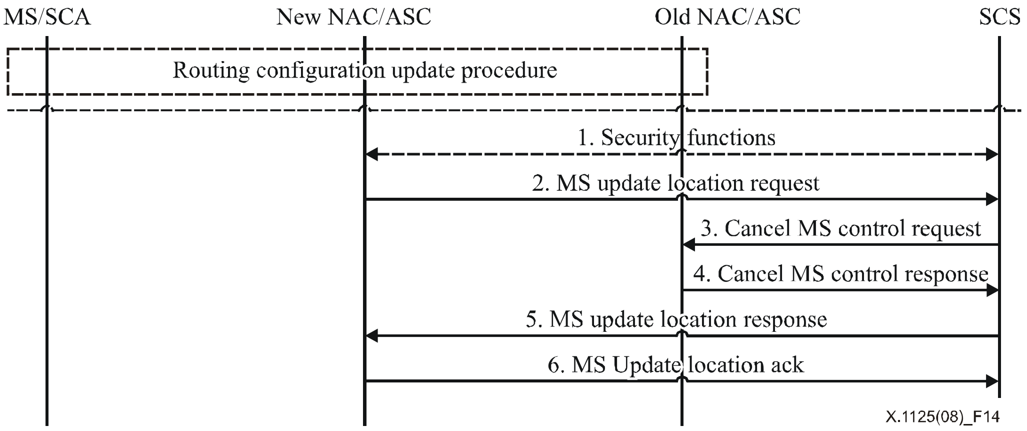

MS/SCA
New NAC/ASC
Old NAC/ASC
SCS
Routing configuration update procedure
1. Security functions
2. MS update location request
3. Cancel MS control request
4. Cancel MS control response
5. MS update location response
6. MS Update location ack
X.1125(08)_F14

Figure 14 – CRS roaming between new NAC/ASC and old NAC/ASC

1) This step is optional and is used for security-related interworking including mutual authentication and the establishment of a secure message transmission tunnel between the new NAC/ASC and the SCS.

2) The new NAC/ASC sends an MS update location request message to the SCS to report the new location of the MS and to request the control policy. The MS update location request message contains information about the identity of the mobile subscriber and of the mobile terminal and the MS addressing information.

3) From the identity of the mobile subscriber that is included in the MS update location request message sent from the new NAC/ASC, the SCS can acquire the old NAC/ASC of the MS. Then the SCS sends a cancel MS control request message to inform the old NAC/ASC that the MS has moved to another area controlled by some other NAC/ASC and the SCS requests it to release the resources applied by CRS and used by the old NAC/ASC to control the MS. The cancel MS control request message contains the identity of the mobile subscriber, the identity of the mobile terminal, and the MS address related information.

4) The old NAC/ASC releases the resources and responds to the cancel MS control response message to the SCS to confirm whether the process is completed.

5) The SCS sends an MS update location response message to the new NAC/ASC and delivers the control policy.

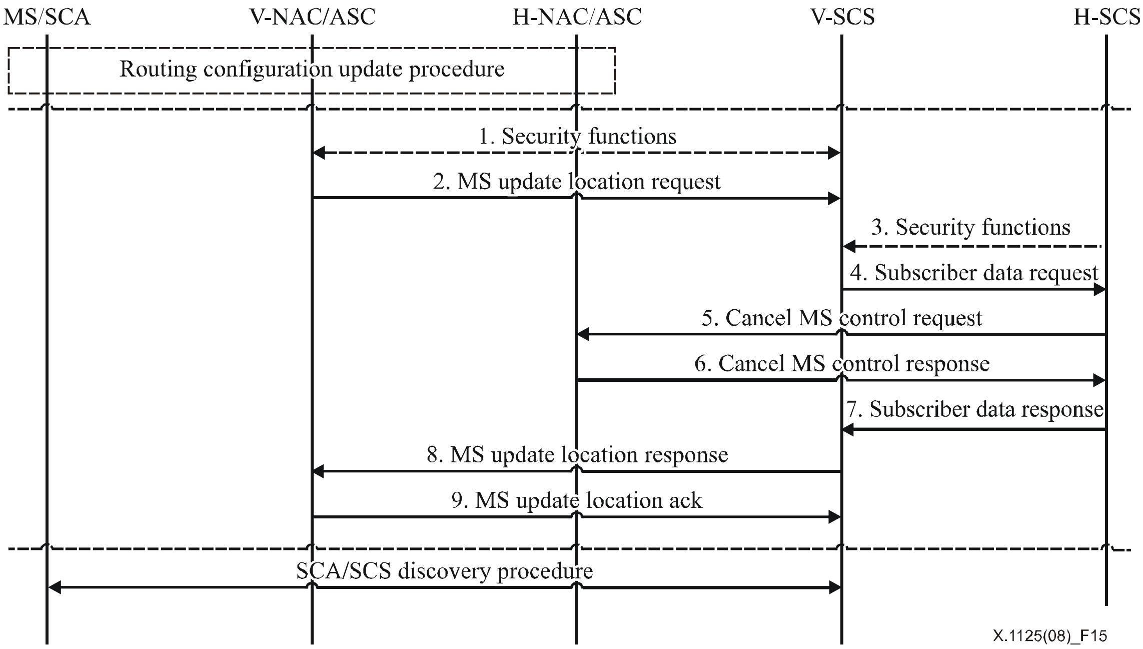
6) The new NAC/ASC returns the enforcement situation of the MS control policy to the SCS.

In the above procedure, the connection between the SCA and the SCS can be maintained.

13.3 CRS roaming between CRS-deployed networks

When the MS roams from one CRS-deployed mobile data network to another, the MS SCA gets the address of the V-SCS and then communicates with it. The V-SCS can get the MS user's information and the MS SCI report to evaluate the security level. However, the V-SCS has no knowledge of the current control policy for the MS user and user-subscribed service, hence the V-SCS needs to request the relevant information from the MS H-SCS.

While the MS roams between two CRS-deployed mobile networks, it needs to implement the MS routing configuration update procedure by interaction among the network devices including the MS, HLR, H-NAC/H-ASC and V-NAC/V-ASC. Meanwhile, the CRS-involved procedure, which is shown in Figure 15, takes place after the V-NAC/V-ASC receives the packet data service information of the MS in the MS routing configuration procedure.



MS/SCA
V-NAC/ASC
H-NAC/ASC
V-SCS
H-SCS
Routing configuration update procedure
1. Security functions
2. MS update location request
3. Security functions
4. Subscriber data request
5. Cancel MS control request
6. Cancel MS control response
7. Subscriber data response
8. MS update location response
9. MS update location ack
SCA/SCS discovery procedure
X.1125(08)_F15

Figure 15 – Inter-roaming between CRS-deployed networks

1) This step is optional and used for security-related interworking including mutual authentication, and for establishing a secure message transport tunnel between the V-NAC/ASC and the V-SCS.

2) The V-NAC/ASC sends the MS update location request message to the V-SCS to report the new location of the MS and to request the control policy. The MS update location request message contains the identity of the mobile subscriber, the identity of the mobile terminal and the packet data service information of the MS.

3) This step is optional and used for security-related interworking including mutual authentication, and for establishing a secure message transport tunnel between the V-SCS and the H-SCS.

4) The V-SCS sends a subscriber data request message to the H-SCS to request information about CRS subscriber customized services and the latest security level of the MS. The subscriber data request message contains the identity of the mobile subscriber and the identity of the mobile terminal.

5) From the identity of the mobile subscriber included in the MS Update Location Request message, the H-SCS can acquire the H-NAC/ASC of the MS. Then the H-SCS sends cancel MS control request message to inform the H-NAC/ASC that the MS has moved to another area controlled by some other V-NAC/ASC and the H-SCS requests it to release the resources applied by the CRS and used by the H-NAC/ASC to control the MS. The cancel MS control request message contains the identity of the mobile subscriber, the identity of mobile terminal and the packet data service information of the MS.

6) The H-NAC/ASC releases the resources after receiving the cancel MS control request message sent from the H-SCS and responds with the cancel MS control response message to the H-SCS to confirm that the process has been completed.

7) The H-SCS sends a subscriber data response message to the V-SCS in response to the information about the user-subscribed CRS services and the latest security level evaluation of the MS. The subscriber data response message contains information on the identity of the mobile subscriber and the identity of the mobile terminal.

8) After the V-SCS analyses the subscriber data response message, the V-SCS sends an MS update location response message to the V-NAC/ASC and delivers the control policy.

9) The V-NAC/ASC returns the implementing status of the MS control policy to the V-SCS.

In the above procedure, the SCA switches to communicate with the V-SCS located in the visited network. Thereafter, the SCA/SCS discovery procedure is initiated by the SCA and the V-SCS.

13.4 CRS roaming between CRS-deployed network and CRS-undeployed network

If the MS home network has deployed CRS but the visited network has not, there are two choices provided for the SCA when the MS roams from the home network to a visited network:

1) The SCA can continue communicating with the H-SCS located in the MS's user home network and only request updating service for the MSOS and the SASs. There is no limitation on the MS to accessing the visited network.

2) Since the visited network has not deployed CRS, the MS SCA turns to an idle state and waits for an activation event. An activation event may be that the MS obtains the address of one of the available SCSs (e.g., according to DHCP protocol or GPRS PDP context activation procedure), or that the MS SCA receives an effective SCA probe request message sent by a SCS.

When the MS roams from one CRS-undeployed wireless data network to CRS-deployed one, the mode of CRS-deployed wireless data network controlling the MS could be:

1) If the MS supports SCA installation, SCA auto-installation can be initiated to install SCA for the MS. Then the network processes the MS SCI reports and wireless data access as per normal CRS procedures.

2) If the MS does not support SCA installation, the CRS-deployed network manages the MS wireless data access according to the operator's own policy. These policies could be:

   i) to filter MS traffic by redirecting to the DSD;

   ii) to limit the user to specific wireless applications provided by the visited network; or

   iii) to forbid the MS to access the wireless data network.

Annex A

CRSAP messages

(This annex forms an integral part of this Recommendation)

A.1 XML schema definition

The XSD specification (see [W3C XSD]) of CRSAP messages is:

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:crsap="urn:oid:0.0.22.1125"
xmlns:crs="urn:oid:0.0.22.1125" targetNamespace="urn:oid:0.0.22.1125"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0" id="CRSAP-
Message">

      <!-- ====================================================================== -->
      <!-- ==========================  CRSAP-Message  =========================== -->
      <!-- ====================================================================== -->

 <element name="CRSAP-Message">
          <complexType>
              <sequence>
                  <element name="Header-Unit" type="crsap:Header-Unit"/>
                  <element name="Body-Unit" type="crsap:Body-Unit"/>
                  <element name="Tail-Unit" type="crsap:Tail-Unit"/>
              </sequence>
          </complexType>
      </element>

      <!-- ======================================================================= -->
      <!-- =============================  Header-Unit  =========================== -->
      <!-- ======================================================================= -->

 <complexType name="Header-Unit">
          <attribute name="Version" type="xs:string" use="required"/>
          <attribute name="Flag" type="crsap:FlagEnumeration" use="required"/>
          <attribute name="Type" type="crsap:TypeEnumeration" use="required"/>
    <attribute name="Precedence" type="xs:nonNegativeInteger" use="required"/>
          <attribute name="Length" type="xs:nonNegativeInteger" use="required"/>
          <attribute name="SCS-ID" type="crsap:ID" use="required"/>
          <attribute name="SCA-ID" type="crsap:ID" use="required"/>
      </complexType>
      <simpleType name="FlagEnumeration">
          <restriction base="xs:string">
              <enumeration value="M">
                  <annotation>
                    <documentation>Multicast message without message tail.</documentation>
                  </annotation>
              </enumeration>
              <enumeration value="MT">
                  <annotation>
                    <documentation>Multicast message with message tail.</documentation>
                  </annotation>
              </enumeration>
              <enumeration value="U">
                  <annotation>
                    <documentation>Unicast message without message tail.</documentation>
                  </annotation>
              </enumeration>
              <enumeration value="UT">
                  <annotation>
                    <documentation>Unicast message with message tail.</documentation>
                  </annotation>
              </enumeration>
          </restriction>
      </simpleType>
      <simpleType name="TypeEnumeration">
          <restriction base="xs:string">
              <enumeration value="U_SCI_Rpt">
                  <annotation>
                    <documentation>Multicast message without message tail.</documentation>
                  </annotation>
              </enumeration>
```

```
            <enumeration value="U_SCA_Prb_Rsp">
                <annotation>
                  <documentation>Multicast message with message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="U_Ack">
                <annotation>
                  <documentation>Unicast message without message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="U_Err_Ntf">
                <annotation>
                  <documentation>Unicast message with message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="D_SCI_Rsp">
                <annotation>
                  <documentation>Multicast message without message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="D_Prb_Req">
                <annotation>
                  <documentation>Multicast message with message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="D_Rep_Req">
                <annotation>
                  <documentation>Unicast message without message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="D_Ack">
                <annotation>
                  <documentation>Unicast message with message tail.</documentation>
                </annotation>
            </enumeration>
            <enumeration value="D_Err_Ntf">
                <annotation>
                  <documentation>Unicast message with message tail.</documentation>
                </annotation>
            </enumeration>
        </restriction>
    </simpleType>

    <!-- ======================================================================== -->
    <!-- ===========================  Body-Unit  ================================ -->
    <!-- ======================================================================== -->

<complexType name="Body-Unit">
        <choice>
            <element name="SCIReport" type="crsap:SCIReportType" />
            <element name="SCIResponse" type="crsap:SCIResponseType" />
            <element name="SCAProbeRequest" type="crsap:SCAProbeRequestType" />
            <element name="SCAProbeResponse" type="crsap:SCAProbeResponseType" />
            <element name="SCIReportRequest" type="crsap:SCIReportRequestType" />
            <element name="Acknowledgement" type="crsap:AcknowledgementType" />
        </choice>
    </complexType>
    <complexType name="SCIReportType">
        <sequence>
            <element name="Rpt_ID" type="xs:string"/>
            <element name="MS_Usr_ID" type="xs:string"/>
            <element name="MS_ISDN" type="xs:string" minOccurs="0"/>
            <element name="MT_ID" type="xs:string"/>
            <element name="MS_OSPlt_TypVer" type="xs:string" minOccurs="0"/>
            <element name="MS_OSPlt_PatLst" type="xs:string" minOccurs="0"/>
            <element name="MS_SAS_Inf" type="xs:string" minOccurs="0"/>
            <element name="MS_Sec_Evt" type="xs:string" minOccurs="0"/>
            <element name="MS_Hrd_Inf" type="xs:string" minOccurs="0"/>
            <element name="SCI_Cur_RptPol" type="xs:string" minOccurs="0"/>
            <element name="SCS_LstCom_Inf" type="xs:string" minOccurs="0"/>
        </sequence>
    </complexType>
    <complexType name="SCIResponseType">
        <sequence>
            <element name="MS_Sec_Lev" type="xs:string" minOccurs="0"/>
            <element name="SCI_New_RptPol" type="xs:string" minOccurs="0"/>
            <element name="SCS_Lmt_Ntf" type="xs:string" minOccurs="0"/>
            <element name="Ack_SCI_Rpt" type="xs:string" minOccurs="0"/>
        </sequence>
    </complexType>
```

```
        <complexType name="SCAProbeRequestType">
            <sequence>
                <element name="SCS_Domain" type="xs:string" minOccurs="0"/>
                <element name="SCS_Address" type="xs:string" minOccurs="0"/>
                <element name="SCS_Port" type="xs:string" minOccurs="0"/>
            </sequence>
        </complexType>
        <complexType name="SCAProbeResponseType">
            <sequence>
                <element name="Lst_SCS_Domain" type="xs:string" minOccurs="0"/>
                <element name="Lst_SCS_Address" type="xs:string" minOccurs="0"/>
                <element name="Lst_SCS_ID" type="xs:string" minOccurs="0"/>
                <element name="Lst_SCA_ID" type="xs:string" minOccurs="0"/>
            </sequence>
        </complexType>
        <complexType name="SCIReportRequestType">
            <sequence>
                <element name="Lst_SCS_Domain" type="xs:string"/>
                <element name="Tim_Rpt" type="xs:string" minOccurs="0"/>
            </sequence>
        </complexType>
        <complexType name="AcknowledgementType">
            <sequence>
                <element name="MsgID_Ack" type="xs:string"/>
            </sequence>
        </complexType>

     <!-- ======================================================================== -->
        <!-- ==========================  Tail-Unit  =============================== -->
        <!-- ======================================================================== -->

    <complexType name="Tail-Unit">
            <sequence>
                <element name="AlgorithmID" type="crsap:ID"/>
                <element name="MsgID" type="crsap:ID"/>
                <element name="MsgDigest" type="crsap:MsgDigest"/>
            </sequence>
        </complexType>
        <simpleType name="ID">
            <restriction base="xs:string">
                <minLength value="1"/>
                <maxLength value="32"/>
            </restriction>
        </simpleType>
        <simpleType name="MsgDigest">
            <restriction base="xs:string">
                <minLength value="8"/>
                <maxLength value="32"/>
            </restriction>
        </simpleType>
</schema>
```

A.2 The equivalent ASN.1 specification of the CRSAP messages

This ASN.1 specification has been generated from the XSD specification, using a tool which conforms to [ITU-T X.694], [ITU-T X.680], [ITU-T X.691] and [ITU-T X.693].

```
X0-0-22-crs {itu-t(0) recommendation(0) x(24) x1125(1125) version1(1) asn1Modules(2) x0-0-22-crs(1)}
DEFINITIONS XER INSTRUCTIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS
    String
    FROM XSD {joint-iso-itu-t asn1(1) specification(0) modules(0) xsd-module(2) version2(2)};

/* ====================================================================== */

/* ==========================  CRSAP-Message  =========================== */

/* ====================================================================== */
CRSAP-Message ::= SEQUENCE {
    header-Unit Header-Unit,
    body-Unit   Body-Unit,
    tail-Unit   Tail-Unit
}
```

```
/* ====================================================================== */

/* =============================  Header-Unit =========================== */

/* ====================================================================== */
Header-Unit ::= SEQUENCE {
    flag       FlagEnumeration,
    length     INTEGER (0..MAX),
    precedence INTEGER (0..MAX),
    sCA-ID     ID,
    sCS-ID     ID,
    type       TypeEnumeration,
    version    XSD.String
}

/* Multicast message without message tail. */

/* Multicast message with message tail. */

/* Unicast message without message tail. */

/* Unicast message with message tail. */
FlagEnumeration ::= ENUMERATED {
    m,
    mT,
    u,
    uT
}

/* Multicast message without message tail. */

/* Multicast message with message tail. */

/* Unicast message without message tail. */

/* Unicast message with message tail. */

/* Multicast message without message tail. */

/* Multicast message with message tail. */

/* Unicast message without message tail. */

/* Unicast message with message tail. */

/* Unicast message with message tail. */
TypeEnumeration ::= ENUMERATED {
    d-Ack,
    d-Err-Ntf,
    d-Prb-Req,
    d-Rep-Req,
    d-SCI-Rsp,
    u-Ack,
    u-Err-Ntf,
    u-SCA-Prb-Rsp,
    u-SCI-Rpt
}

/* ====================================================================== */

/* ===========================  Body-Unit  ============================== */

/* ====================================================================== */
Body-Unit ::= SEQUENCE {
    choice CHOICE {
        sCIReport        SCIReportType,
        sCIResponse      SCIResponseType,
        sCAProbeRequest  SCAProbeRequestType,
        sCAProbeResponse SCAProbeResponseType,
        sCIReportRequest SCIReportRequestType,
        acknowledgement  AcknowledgementType
    }
}

SCIReportType ::= SEQUENCE {
    rpt-ID          XSD.String,
    mS-Usr-ID       XSD.String,
    mS-ISDN         XSD.String OPTIONAL,
    mT-ID           XSD.String,
    mS-OSPlt-TypVer XSD.String OPTIONAL,
    mS-OSPlt-PatLst XSD.String OPTIONAL,
    mS-SAS-Inf      XSD.String OPTIONAL,
    mS-Sec-Evt      XSD.String OPTIONAL,
    mS-Hrd-Inf      XSD.String OPTIONAL,
    sCI-Cur-RptPol  XSD.String OPTIONAL,
    sCS-LstCom-Inf  XSD.String OPTIONAL
}

SCIResponseType ::= SEQUENCE {
    mS-Sec-Lev     XSD.String OPTIONAL,
    sCI-New-RptPol XSD.String OPTIONAL,
    sCS-Lmt-Ntf    XSD.String OPTIONAL,
    ack-SCI-Rpt    XSD.String OPTIONAL
}

SCAProbeRequestType ::= SEQUENCE {
    sCS-Domain  XSD.String OPTIONAL,
    sCS-Address XSD.String OPTIONAL,
    sCS-Port    XSD.String OPTIONAL
}

SCAProbeResponseType ::= SEQUENCE {
    lst-SCS-Domain  XSD.String OPTIONAL,
    lst-SCS-Address XSD.String OPTIONAL,
    lst-SCS-ID      XSD.String OPTIONAL,
    lst-SCA-ID      XSD.String OPTIONAL
}

SCIReportRequestType ::= SEQUENCE {
    lst-SCS-Domain XSD.String,
    tim-Rpt        XSD.String OPTIONAL
}

AcknowledgementType ::= SEQUENCE {
    msgID-Ack XSD.String
}

/* ====================================================================== */
/* ===========================  Tail-Unit =============================== */
/* ====================================================================== */
Tail-Unit ::= SEQUENCE {
    algorithmID ID,
    msgID       ID,
    msgDigest   MsgDigest
}

ID ::= XSD.String (SIZE(1..32))

MsgDigest ::= XSD.String (SIZE(8..32))

ENCODING-CONTROL XER
    GLOBAL-DEFAULTS MODIFIED-ENCODINGS
    GLOBAL-DEFAULTS CONTROL-NAMESPACE
       "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
    NAMESPACE ALL, ALL IN ALL AS "urn:oid:0.0.22.crs" PREFIX "crsap"
    NOT NAMESPACE Header-Unit.flag, Header-Unit.length,
       Header-Unit.precedence, Header-Unit.sCA-ID, Header-Unit.sCS-ID,
       Header-Unit.type, Header-Unit.version
    NAME CRSAP-Message.header-Unit, CRSAP-Message.body-Unit,
       CRSAP-Message.tail-Unit, Header-Unit.flag, Header-Unit.length,
       Header-Unit.precedence, Header-Unit.sCA-ID, Header-Unit.sCS-ID,
       Header-Unit.type, Header-Unit.version, Body-Unit.choice.sCIReport,
       Body-Unit.choice.sCIResponse, Body-Unit.choice.sCAProbeRequest,
       Body-Unit.choice.sCAProbeResponse, Body-Unit.choice.sCIReportRequest,
       Body-Unit.choice.acknowledgement, Tail-Unit.algorithmID,
       Tail-Unit.msgID, Tail-Unit.msgDigest AS CAPITALIZED
    NAME SCIReportType.rpt-ID AS "Rpt_ID"
    NAME SCIReportType.mS-Usr-ID AS "MS_Usr_ID"
    NAME SCIReportType.mS-ISDN AS "MS_ISDN"
    NAME SCIReportType.mT-ID AS "MT_ID"
    NAME SCIReportType.mS-OSPlt-TypVer AS "MS_OSPlt_TypVer"
    NAME SCIReportType.mS-OSPlt-PatLst AS "MS_OSPlt_PatLst"
    NAME SCIReportType.mS-SAS-Inf AS "MS_SAS_Inf"
    NAME SCIReportType.mS-Sec-Evt AS "MS_Sec_Evt"
    NAME SCIReportType.mS-Hrd-Inf AS "MS_Hrd_Inf"
    NAME SCIReportType.sCI-Cur-RptPol AS "SCI_Cur_RptPol"
    NAME SCIReportType.sCS-LstCom-Inf AS "SCS_LstCom_Inf"
    NAME SCIResponseType.mS-Sec-Lev AS "MS_Sec_Lev"
    NAME SCIResponseType.sCI-New-RptPol AS "SCI_New_RptPol"
    NAME SCIResponseType.sCS-Lmt-Ntf AS "SCS_Lmt_Ntf"
    NAME SCIResponseType.ack-SCI-Rpt AS "Ack_SCI_Rpt"
    NAME SCAProbeRequestType.sCS-Domain AS "SCS_Domain"
    NAME SCAProbeRequestType.sCS-Address AS "SCS_Address"
    NAME SCAProbeRequestType.sCS-Port AS "SCS_Port"
    NAME SCAProbeResponseType.lst-SCS-Domain AS "Lst_SCS_Domain"
    NAME SCAProbeResponseType.lst-SCS-Address AS "Lst_SCS_Address"
    NAME SCAProbeResponseType.lst-SCS-ID AS "Lst_SCS_ID"
    NAME SCAProbeResponseType.lst-SCA-ID AS "Lst_SCA_ID"
    NAME SCIReportRequestType.lst-SCS-Domain AS "Lst_SCS_Domain"
    NAME SCIReportRequestType.tim-Rpt AS "Tim_Rpt"
    NAME AcknowledgementType.msgID-Ack AS "MsgID_Ack"
    ATTRIBUTE ALL IN Header-Unit
    UNTAGGED Body-Unit.choice
    TEXT FlagEnumeration:ALL AS CAPITALIZED
    TEXT TypeEnumeration:d-Ack AS "D_Ack"
    TEXT TypeEnumeration:d-Err-Ntf AS "D_Err_Ntf"
    TEXT TypeEnumeration:d-Prb-Req AS "D_Prb_Req"
    TEXT TypeEnumeration:d-Rep-Req AS "D_Rep_Req"
    TEXT TypeEnumeration:d-SCI-Rsp AS "D_SCI_Rsp"
    TEXT TypeEnumeration:u-Ack AS "U_Ack"
    TEXT TypeEnumeration:u-Err-Ntf AS "U_Err_Ntf"
    TEXT TypeEnumeration:u-SCA-Prb-Rsp AS "U_SCA_Prb_Rsp"
    TEXT TypeEnumeration:u-SCI-Rpt AS "U_SCI_Rpt"
END
```

Appendix I

Some considerations on CRS implementation

(This appendix does not form an integral part of this Recommendation)

I.1 Deployment of SCA

I.1.1 Installation or distribution of SCA software

In most cases, the initial installation of SCA should be achieved by the SCA auto-installation procedure. However, there may be other methods to do that. The methods are listed as follows:

– Auto-installation of SCA

  Initially, the MS does not install the SCA. When the MS accesses a CRS-deployed wireless data network, the MS finishes the installation and initialization of SCA relying on the SCA auto-installation procedure that is specified in clause 11.3.1.

– As a component, the SCA is embedded in a mobile terminal

  MS or MSOS manufacturers embed the SCA with the latest version in the MS before its delivery to the MS user, i.e., the SCA is a pre-installed component of the MS. Or SCA can be installed on the MS together with the installation of SAS and SCA acts as a component of the SAS software.

– As a component, the SCA is embedded into a smart card of MS

  Card manufacturers embed the SCA with the latest version in the card before its delivery to the mobile user, i.e., the SCA is a pre-installed component of the smart card. By the methods of purchasing the smart card or changing the smart card, the SCA can be distributed to end users.

SCA installation and SCA re-installation should be handled as a single transaction, i.e., if the SCA installation fails before completion for some reason (e.g., abnormal power-off of the MS or SCA installation process killed by the user), the installation procedure can be rolled back to the state when the SCA installation is to be started.

Succeeding updates of the SCA rely on the SCA auto-updating procedure specified in clause 11.3.2.

I.1.2 Embedding location of SCA software

The possible embedded locations of SCA software may be as follows:

– MS storage media area

  The SCA is installed in the MS storage media as independent software of the MS. In this case, the SCA installation program should limit the SCA to be installed in the fixed storage media area only. To ensure SCA works continuously and reliably, removable storage media is not recommended (so that the abnormity caused by the change of storage media and further SCA auto-installation can be avoided).

– Embedded in the SAS

  The SCA is integrated into the security application software on the MS as one integral component. In that case, the SCA communicates with the MSOS or other SAS via the interfaces between the MSOS and SAS. The information contents exchanged in these interfaces are the same as those in the messages via *Ica*. The communication between the SCA module and the SAS falls into the internal information-exchange process. Also see the following Figure I.1.

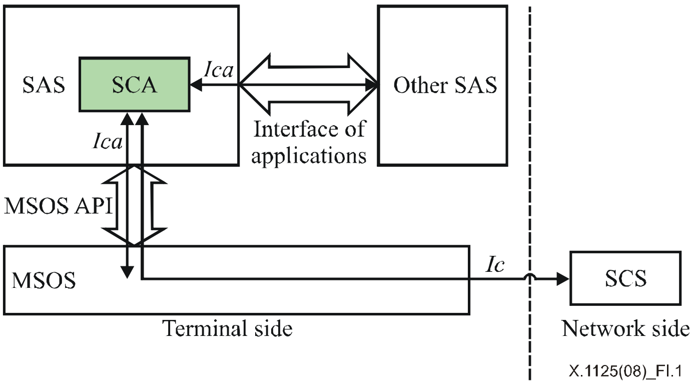


Figure I.1 – SCA deployed in SAS

As can be seen from Figure I.1, the interface between MSOS and SAS and the one between SAS and the other SAS are MSOS API or application program interfaces that MSOS opens for upper-layer applications. The information transmitted between the two interfaces is specified by clause 7.5, which primarily includes the security-related information of the MSOS and SAS. Therefore, from the view of the application layer, the MSOS API, as one information carrier channel, achieve the function of *Ica*.

– Embedded in user smart card

The SCA acts as an updatable application program of the smart card as shown in Figure I.2.

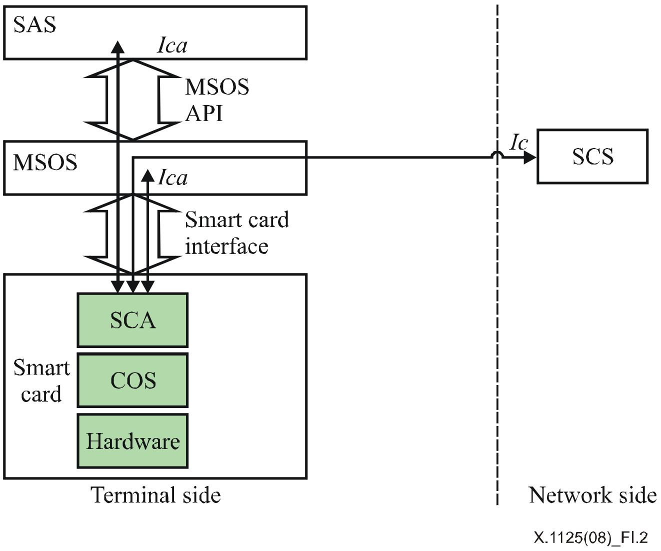


Figure I.2 – SCA deployed in smart card

As shown in Figure I.2, the actual interface between the SAS and MSOS is the smart card interface and MSOS API opened for upper-layer applications. As the *Ica* message-carrying tunnel, the MSOS API and smart card interface provides the transportation for *Ica* messages. According to the interfaces specified in [b-ETSI TS 102 223], the data exchange between the smart card and terminal can be implemented using TCP/IP.

I.2 Deployment of SCS

In CRS, the SCS communicates with the MS, access device of the core network, gateway device in the core network and servers on the Internet/PDN.

– the SCS communicates with the MS and servers on the Internet/PDN

  The data which the SCS communicates with the MS and servers on the Internet/PDN are firstly encapsulated by the tunnel protocol, then transmitted in the CN. These data are encapsulated/decapsulated at the edge of the CN and in the SCS.

– The SCS communicates with the network access device and gateway device

  The SCS communicates with network access device (such as the NAC in CRS architecture) and gateway device of the CN. The communication data can be encapsulated as the payload of the IP layer of the CN and transmitted directly upon the IP layer of the CN, they can also be encapsulated as the payload in a tunnel between the communication peers.

In CRS, there are two main methods for the deployment of SCS:

– Deployment of one suite of SCS in a PLMN/CN is a common use case. This suite of SCS serves for all MSs that access any PDN connected with the PLMN/CN.

  The PLMN's sketch map is described in Figure I.3 when deploying one suite of SCS in a PLMN/CN, the broken line indicates which PDN or Internet the SCS serves.

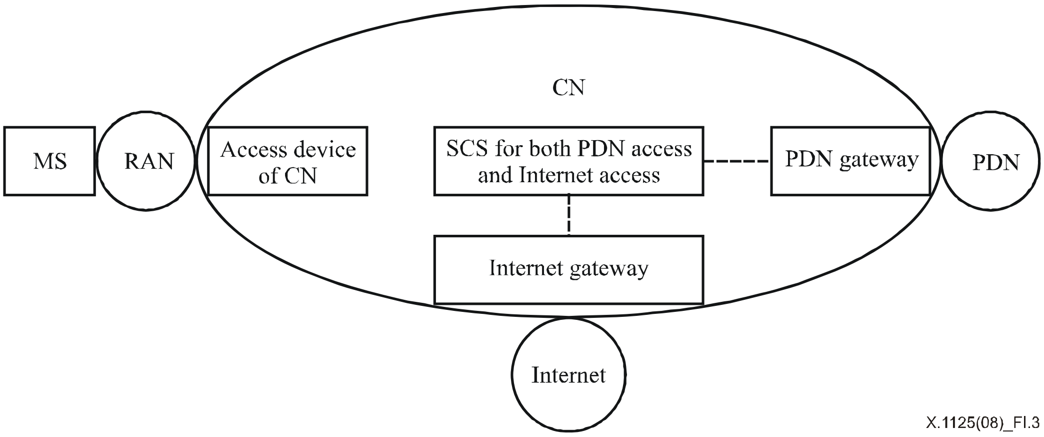


Figure I.3 – One PLMN/CN deploys one suite of SCS

See clause 7.4.2.2 for SCS's protocol stack structure when deploying one suite of SCS in a PLMN/CN.

– Deploying more than one suite of SCS in a PLMN/CN is another use case derived from the above-mentioned one. In this use case, each suite of SCS serves for MSs who access certain PDN or PDNs connected with the PLMN/CN.

  The PLMN's sketch map is shown in Figure I.4 when deploying one suite of SCS for each PDN connected to PLMN/CN, the broken line indicates which PDN or Internet the SCS serves.

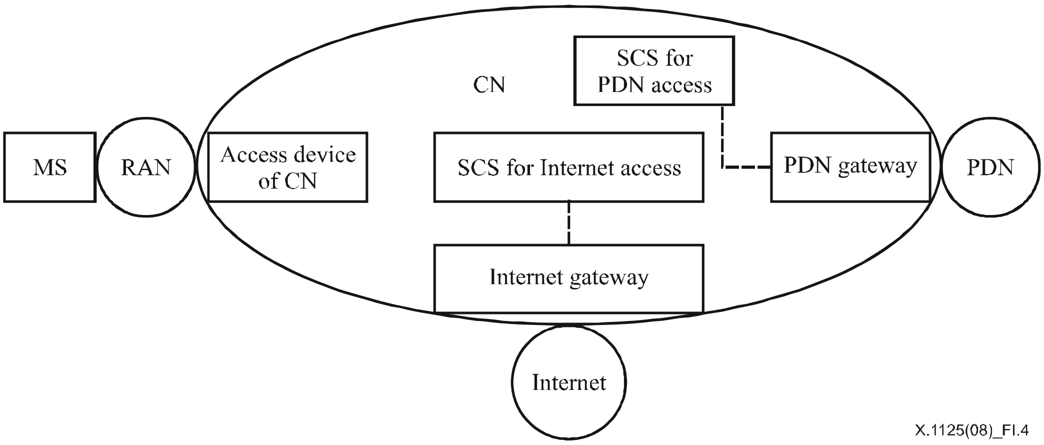


Figure I.4 – Deployment of one suite of SCS for each PDN connected to PLMN/CN

The SCS's protocol stack structure is as shown below in Figure I.5 when deploying one suite of SCS for each PDN connected to PLMN/CN.

<table>
<tr><td rowspan="4">Upper layer protocol/ application</td><td colspan="2">Upper layer protocol/application</td></tr>
<tr><td colspan="2">Transport layer protocol (TCP/UDP)</td></tr>
<tr><td>IP
(for PDN 1)</td><td>IP
(for Internet)</td></tr>
<tr><td colspan="2">Tunnel protocol</td></tr>
<tr><td colspan="3">Transport layer protocol (TCP/UDP)</td></tr>
<tr><td colspan="3">IP (for CN)</td></tr>
<tr><td colspan="3">L1 and L2 protocols</td></tr>
</table>

SCS protocol stack
(serves PDN 1)

<table>
<tr><td rowspan="4">Upper layer protocol/ application</td><td colspan="2">Upper layer protocol/application</td></tr>
<tr><td colspan="2">Transport layer protocol (TCP/UDP)</td></tr>
<tr><td>IP
(for PDN 2)</td><td>IP
(for Internet)</td></tr>
<tr><td colspan="2">Tunnel protocol</td></tr>
<tr><td colspan="3">Transport layer protocol (TCP/UDP)</td></tr>
<tr><td colspan="3">IP (for CN)</td></tr>
<tr><td colspan="3">L1 and L2 protocols</td></tr>
</table>

SCS protocol stack
(serves PDN 2)

Figure I.5 – SCS protocol stack structure
(deploy one suite of SCS for each PDN connected to PLMN/CN)

When deploying one suite of the SCS for each PDN connected to PLMN/CN, each SCS has a static IP address (IP for PDN) associated with the PDN above the layer of the tunnel protocol. This IP address is used by the SCS (serves corresponding PDN) to communicate with MSs or network elements, which access (or exist in) the associated PDN. The SCS may also have a static IP address above the layer of the tunnel protocol, which is used by the SCS to access Internet resources.

The term 'PDN' mentioned above refers to the packet data network, thus the Internet is also one kind of PDN. However, to make it easy to comprehend, the Internet is depicted in Figure I.5 separately from the PDN. Here, a suite of SCS means one or more SCSs, which have the same function and protocol stack structure, i.e., a suite of SCS contains at least one SCS in the normal operating state and one or more SCSs in the backup state.

I.3 Deployment of CRS in mobile IP networks

If CRS is deployed together with mobile IP, there are two considerations for the CRS operation mode:

1) For mobile IP, during the period of roaming, the mobile node can be addressed without changing its IP address, resulting in that user's application being uninterrupted and thus the mobile node seems to be located in its home network. Therefore, the MS can still utilize various configurations applied in its home network, including the SCS and NAC. The MS security level is evaluated and determined by the H-SCS, and all control on MSs is enforced by the H-NAC/ASC.

2) Considering the utilization efficiency of the mobile network, the MS can communicate with the V-SCS by using its care-of-address assigned by the visited network. The MS security level is evaluated and determined by the V-SCS, and all control on MSs is enforced by the V-NAC/ASC.

Appendix II

An example of CRSAP message exchange

(This appendix does not form an integral part of this Recommendation)

II.1 An example SCI report

One mobile phone accessing GPRS network with Symbian S60 OS, mobile user ID: 0413559827.

When the SCA (SCA ID: 7056487) detects that the mobile is infected by "Qdial.A.Trojan" and the Trend AV software cannot kill it, the SCA is triggered to send an SCI report for this security event to the SCS (SCS ID:4041).

An XML encoding (conforming to Annex A) for a possible SCI report could be:

```
<?xml version="1.0" encoding="UTF-8"?>
<CRSAP-Message   xmlns="urn:oid:0.0.22.crs"   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oid:0.0.22.crs crsap.xsd">

        <Header-Unit  Type="U_SCI_Rpt"  Precedence=”4”  Length="8"  SCA-ID="7056487"  Flag="UT"  SCS-
ID="4041" Version="1.0"/>

    <Body-Unit>
          <SCIReport>
             <Rpt_ID>017</Rpt_ID>
             <MS_Usr_ID>0413559827</MS_Usr_ID>
        <MT_ID>356412018613007</MT_ID>
        <MS_OSPlt_TypVer> Symbian S60</MS_OSPlt_TypVer>
        <MS_Sec_Evt>Infected by “Qdial.A.Trojan”.</MS_Sec_Evt>
        <SCI_Cur_RptPol>401</SCI_Cur_RptPol>
        </SCIReport>
        </Body-Unit>

    <Tail-Unit>
            <AlgorithmID>SHA1-128</AlgorithmID>
            <MsgID>0112</MsgID>
            <MsgDigest>7B64AC21</MsgDigest>
        </Tail-Unit>
</CRSAP-Message>
```

II.2 An example SCI response

After receiving the report, the SCS changed the security level of the MS from level 2 (low aggressiveness and medium vulnerability) to level 6 (i.e., high aggressiveness and medium vulnerabilitity), and sent an SCI response to inform the SCA of the change and to indicate the SCA enforcing SCA control policy number 403 (i.e., to shorten the report period).

```
<?xml version="1.0" encoding="UTF-8"?>
<CRSAP-Message   xmlns="urn:oid:0.0.22.crs"   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oid:0.0.22.crs crsap.xsd">

        <Header-Unit  Type="D_SCI_Rsp"  Precedence=”4”  Length="8"  SCA-ID="7056487"  Flag="UT"  SCS-
ID="4041" Version="1.0"/>

    <Body-Unit>
          <SCIResponse>
                <MS_Sec_Lev>Level 6<MS_Sec_Lev>
                <SCI_New_RptPol>403<SCI_New_RptPol />
        </SCIResponse >
        </Body-Unit>

    <Tail-Unit>
            <AlgorithmID>SHA1-128</AlgorithmID>
            <MsgID>0113</MsgID>
            <MsgDigest>6A457B1C</MsgDigest>
        </Tail-Unit>
</CRSAP-Message>
```

Bibliography

[b-3GPP Network] 3GPP TS 23.002 V7.1.0 (2006), *Network Architecture.*
<http://www.3gpp.org/ftp/specs/html-info/23002.htm>

[b-3GPP GPRS] 3GPP TS 23.060 V7.0.0 (2006), *General Packet Radio Service (GPRS); Service description; Stage 2*.
<http://www.3gpp.org/FTP/Specs/html-info/23060.htm>

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol.*
<http://www.ietf.org/rfc/rfc2131.txt>

[b-IETF RFC 2903] IETF RFC 2903 (2000), *Generic AAA Architecture.*
<http://www.ietf.org/rfc/rfc2903.txt>

[b-IETF RFC 2904] IETF RFC 2904 (2000), *AAA Authorization Framework.*
<http://www.ietf.org/rfc/rfc2904.txt>

[b-IETF RFC 2905] IETF RFC 2905 (2000), *AAA Authorization Application Examples.*
<http://www.ietf.org/rfc/rfc2905.txt>

[b-IETF RFC 2906] IETF RFC 2906 (2000), *AAA Authorization Requirements.*
<http://www.ietf.org/rfc/rfc2906.txt>

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR).*
<http://www.ietf.org/rfc/rfc3084.txt>

[b-IETF RFC 3470] IETF RFC 3470 (2003), *Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols.*
<http://www.ietf.org/rfc/rfc3470.txt>

[b-IETF RFC 4261] IETF RFC 4261 (2005), *Common Open Policy Service (COPS) Over Transport Layer Security (TLS).*
<http://www.ietf.org/rfc/rfc4261.txt>

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*
<http://www.ietf.org/rfc/rfc4301.txt>

[b-IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1.*
<http://www.ietf.org/rfc/rfc4346.txt>

[b-ETSI TS 102 223] ETSI TS 102 223 (2008), *Smart Cards; Card Application Toolkit (CAT) (Release 8).*
<http://pda.etsi.org/pda/home.asp?wki_id=lxYe5I0QA1@.22.03WR-G>

[b-OASIS AVDL] OASIS AVDL (2004), *Application Vulnerability Description Language (AVDL) v1.0.*
<www.oasis-open.org/committees/avdl/>

[b-OMA WTLS] OMA Release WTLS (2001), *Wireless Transport Layer Security Version 06-Apr-2001.*
<http://www.openmobilealliance.org/tech/affiliates/wap/wap-261-wtls-20010406-a.pdf>

[b-OSVDB] Open Source Vulnerability Database, <http://www.osvdb.org>.

[b-W3C XML] W3C Recommendation XML (2004), *Extensible Markup Language (XML) 1.0 (Third Edition).*
<http://www.w3.org/TR/2004/REC-xml-20040204/>

[b-W3C Datatypes] W3C Recommendation Datatypes (2004), *XML Schema Part 2: Datatypes Second Edition.*
<http://www.w3.org/TR/xmlschema-2/>

[b-W3C Namespace] W3C Recommendation Namespaces (2006), *Namespaces in XML 1.0 (Second Edition).*
<http://www.w3.org/TR/REC-xml-names/>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008