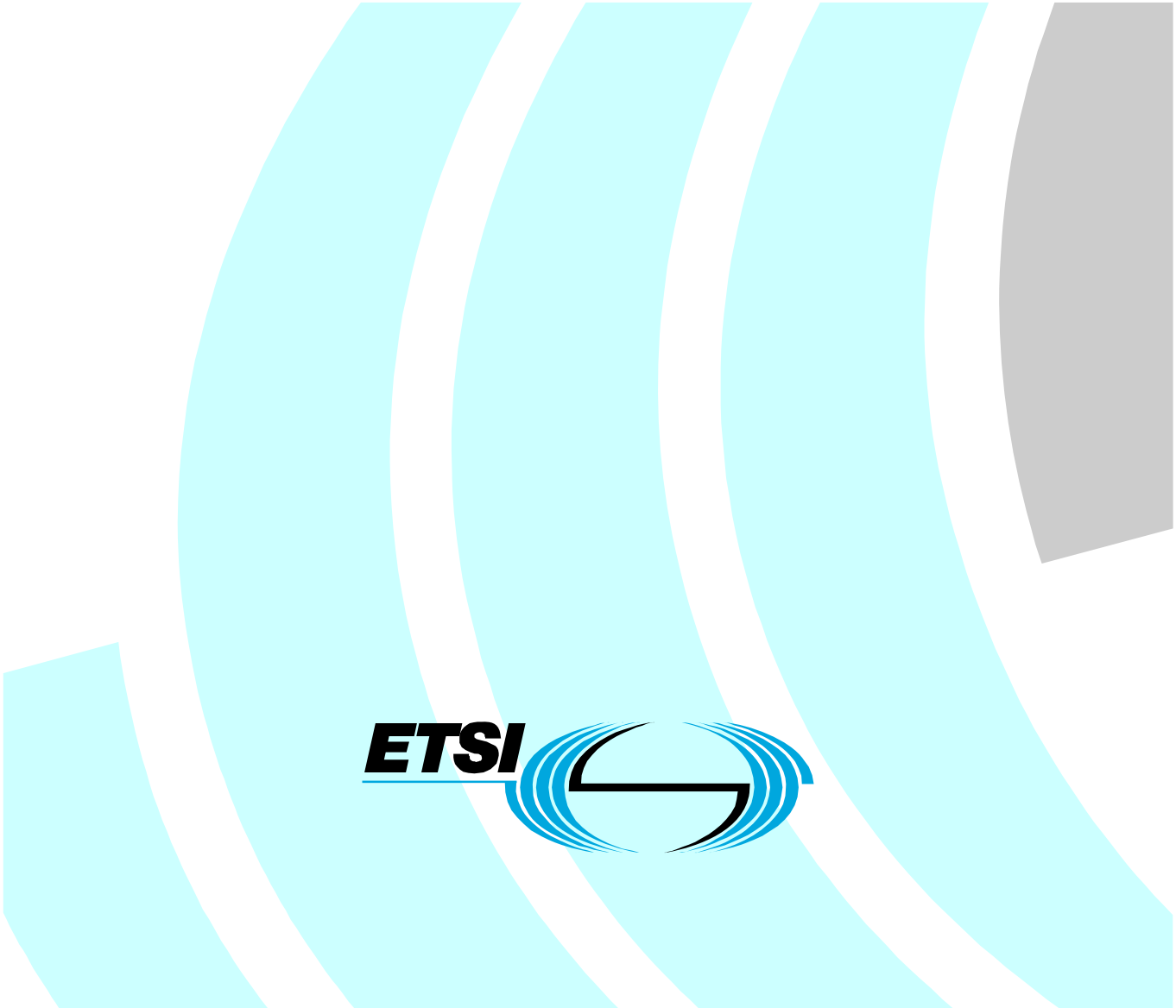
ETSI TR 185 008 V2.0.0 (2008-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of security mechanisms for customer networks connected to TISPAN NGN R2



Reference
DTR/TISPAN-05017-NGN-R2

Keywords
authentication, gateway, network, service, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document present an analysis of the security mechanisms that could be supported in the customer environment (Customer Network Gateway or Customer Devices) with reference to the overall end to end security architecture for the NGN defined by WG7. As examples, these mechanisms can be related to authentication (for connectivity and for services), firewalling and network access/parental control, virus protection, intrusion detection, Anti Spam capabilities. The activity will be performed in close relationship with WG7.

The reactions to threats or the protections against threats described in the present document will involve only the CPN, not the external network.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

None.

2.2 Informative references

[1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[2] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (Release 7) (3GPP TR 21.905)".

[3] ISO/IEC 7498-2: "Information Processing Systems - Interconnection Reference Model - Part 2: Security Architecture".

[4] draft-ietf-nea-requirements-04.txt, Network Endpoint Assessment (NEA): "Overview and Requirements", August 2007.

[5] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security".

[6] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services".

[7] ETSI TS 133 246: "Universal Mobile Telecommunications System (UMTS); 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[8] ETSI TS 133 110: "Universal Mobile Telecommunications System (UMTS); Key establishment between a UICC and a terminal".

[9] ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

[10] ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN Customer Devices architecture and interfaces".

[11] ETSI TR 187 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report".

[12] IETF RFC 1827: "IP Encapsulating Security Payload (ESP)".

[13] IEEE 802.11a: "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band".

[14] IEEE 802.11b: "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band".

[15] IEEE 802.11i: "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements".

[16] IEEE 802.11g: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band".

[17] ETSI TR 187 009: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Feasibility study of prevention of unsolicited communication in the NGN".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authentication: property by which the correct identity of an entity or party is established with a required assurance.The party being authenticated could be a user, subscriber, home environment or serving network (see TR 121 905 [2])

authorization: granting of permission based on authenticated identification (see ISO/IEC 7498-2 [3])

NOTE: In some contexts, authorization may be granted without requiring authentication or identification e.g. emergency call services.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
AV	Anti-Virus
CND	Customer Network Device
CNG	Customer Network Gateway
CPN	Customer Premises Network
EAP	Extensible Authentication Protocol
FMCA	Fixed-Mobile Convergence Alliance
IDS	Intrusion Detection System
IMS	IP Multimedia subsystem
IPSEC	Internet Protocol SECurity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MMS	Multimedia Messaging Service
MPLS	Multiple Protocol Label Switching
NAC	Network Access Control
NAT	Network Address Translation
NEA	Network Endpoint Assessment
P-CSCF	Proxy-Call Session Control Function
PDA	Personal digital assistant
RTP	Real-time Transport Protocol
SMS	Short Message Service
SSL	Secure socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UC	Unsolicited Communication
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTM	Unified Threat Management
VPN	Virtual Private Network
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WPA2	Wi-Fi Protected Access 2

4 CPN Reference Architecture

A typical example of architecture could be the following one, where several types of devices are connected to the CNG. Of course, there could be several of each type.

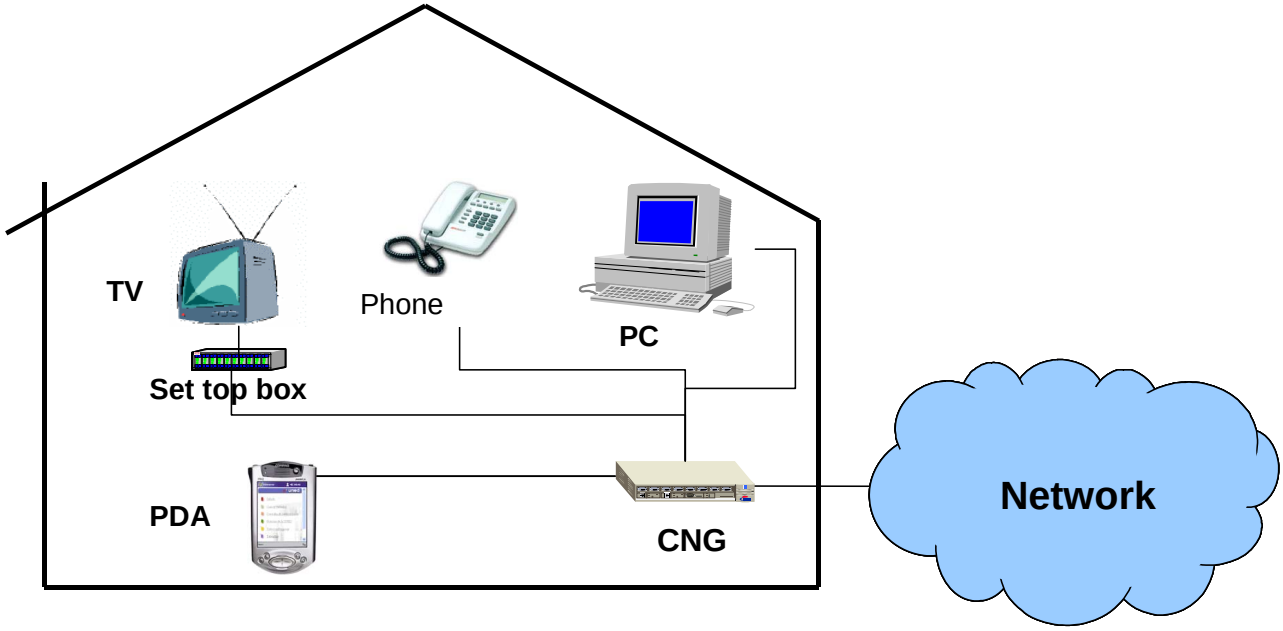


Figure 1: Example of CNP architecture

5 Main security threats and security recommendations

Considering the CPN, security problems can have two origins. They can be originated from inside the CPN, or from outside the CPN. The external origin itself can be sub-divided into two parts, the legitimate network to which the CPN is connected, or a non legitimate network to which the CPN can be accidentally connected (e.g. WLAN).

Threats on security can be categorized with the following:

- System/device integrity: case of the virus attack, malware.
- Unsolicited information: it can be either spam problems (can lead to device integrity problem in case of virus transmission) or display of text, pictures, video, not initially requested by the customer.
- Unauthorized access: this could either be an external third party accessing the CPN (and using it to access services through the CNG), or someone authorized to access an use the CPN but accessing unauthorized data in the network (e.g. children accessing adult content).
- Confidentiality: private data can be protected from interception during communication, or from being stolen (due to spyware or unauthorized access).
- Service availability: contains all the actions that would lead to a DoS.
- Masquerade: this term covers all the possibilities for a spoofing attack as already known on the Internet. This is mainly man-in-the-middle attack and internet protocol spoofing, URL spoofing and phishing, referer spoofing, poisoning of file-sharing networks, caller ID spoofing, e-mail address spoofing, login spoofing.

The starting point for security recommendations is the following already existing security requirements found in TS 185 005 [9]:

- [The CNG shall support mechanisms to authenticate itself to the NGN for connectivity purposes.
- The CNG shall support mechanisms to authenticate itself to the NGN for service usage purposes.

- The CNG shall support mechanisms to authenticate CNDs to the NGN for service usage purposes if they are not able to fully support the related procedures in an autonomous way.
- The CNG shall support mechanisms for authentication of wireless CNDs for local connectivity. Similar mechanisms may be also implemented for non-wireless devices.
- The CNG and CPN shall support mechanisms that prevent access to the network by unauthorized users.
- The capacity of the authorized entities should depend on the security policies defined by the service providers, managing the CNG.
- The CNG and the CPN shall implement mechanisms to limit the visibility of the WAN side network and resources to authorized entities.
- The diagnostic operations on the CPN by an operator shall be performed in accordance with rules protecting the users' privacy.
- CPN environment shall be protected with a stateful firewall function, which may be implemented in the CNG.
- The CNG and the CPN shall be able to support parental control related functionalities limiting the use of the broadband connection on a user or time basis. Limitations on a content basis may be shared with devoted network servers.]

The following recommendation is proposed to enhance the above existing security requirements defined in TS 185 005 [9] (WI05014):

- A mechanism to allow and manage different levels of user's rights can be implemented.

6 Security mechanisms for Customer Premises Network

Depending on the various threats and their large abilities to disrupt the CPN, several security mechanisms should be taken into account.

The CPN environment also hosts several kinds of users: families with children, teleworkers, friends and neighbours and so on. Each users could be the target (or the source) of specific threats and hence may require specific security mechanisms (i.e. VPN for teleworkers, parental control for children, etc.).

6.1 Authentication and authorization mechanisms

Security threats addressed:

- masquerade;
- unauthorized;
- access.

Level of action in the CPN: gateway authentication and authorization, device authentication, user authentication and authorization, message authentication, authentication and authorization of a user for access to a service or set of services, and authentication of the network and/or service provider.

- CNG authentication: connectivity authentication towards the Network Domain Security.
- CND authentication: local authentication towards the local access point (e.g. Wi-Fi access point) embedded in the gateway. Methods to establish shared keys for authentication are proposed within TS 133 110 [8] and TS 133 246 [7].
- User authentication: to access service platform in general.
- Message and Service authentication: to access a specific service/application.

NOTE: In the relation to the four authentication methods mentioned above further investigations are needed and will be carried out by WG5 and WG7 to clearly specify the accurate roles for CNG and CND in supporting the mechanisms.

The basis of identification may be one or more of the following:

- Something the entity knows such as passwords or keys.
- Something the entity possesses such as UICC or hardware token improving the security of authentication mechanisms.
- Something inherent to the entity such as fingerprints or retinal characteristics.

The preferred method for user and service authentication is IMS-AKA. To fully implement the IMS-AKA framework, a UICC is needed into the CPN device which is terminating the IMS security association.

To be compliant with TS 187 001 [1], there are other two methods to be considered: Http Digest and NBA.

The mechanisms for the user's authentication in the TISPAN context are enablers for legacy terminals to access the IMS services. In that sense, IMS-AKA and HTTP Digest should be supported by the CNG and may be supported by CNDs. If not supported by CNDs, the CNG can play an active role in completing the procedure, as also described in TS 185 006 [10].

6.1.1 Wireless security mechanisms

Security threats addressed:

- unauthorized access;
- breach of system/device integrity;
- breach of confidentiality.

Level of action in the CPN: CNG, CND.

Wireless communications technologies are widely adopted and very common both for large organizations and customer environments. The most popular technologies are based on the IEEE standards, such as the 802.11a/b/g [13], [14], [16]. The interoperability certification for IEEE 802.11x WLANs is Wireless Fidelity (Wi-Fi) and is controlled by the Wi-Fi Alliance (WFA). Also work with Fixed-Mobile Convergence Alliance (FMCA) is being carried out on setting requirements for both device access points and network gateways to support service applications on the scope of the present document.

However, wireless networking has many security issues that cannot be ignored, even in a customer environment. The IEEE 802.11b [14] protocol is the most commonly deployed wireless protocol, and although it has the ability to use 64-bit or 128-bit encryption, readily available software can crack the encryption scheme. To overcome the security weakness present in the WLAN environment, the IEEE 802.11i [15] standard was ratified to provide additional security in WLAN networks.

IEEE 802.11i [15] is also known as Wi-Fi Protected Access 2 (WPA2). The 802.11i [15] architecture is based on the following main components:

- 802.1X for authentication (based on the Extensible Authentication Protocol).
- Advanced Encryption Standard (AES) as the encryption method.

By 2006, the WPA2 certification became mandatory for all new equipment certified by the Wi-Fi alliance. Home Gateway Initiative (HGI) also endorsed WFA guidelines and requires WPA2 certification for the wireless access points installed in home gateways (CNGs). WAP2 certified products are supporting WPA for backward compatibility reason.

6.2 Security Management functionality

Security threats addressed:

- unauthorized access;
- breach of system/device integrity.

Level of action in the CPN: CNG, CNDs Security management functionality addresses both local and remote access security.

For the local security, it will control all the local exchanges between the devices inside the CPN.

Concerning external security, this will cover the cases of remote management, both from the user (e.g. remote activation of a VCR, remote control of a camera, etc.) or from the network provider (e.g. remote update of the gateway's network data).

These security tasks may be accomplished with the support of additional features, like the authentication features embedded in some chipsets (Trusted Platform Module) or UICC inserted in the CNG that may contain credentials, security algorithms and also other configuration parameters (e.g. some policy rules for the firewall).

6.3 Firewall

Security threats addressed:

- unauthorized access;
- breach of system/device integrity;
- initiation of unsolicited information;
- breach of confidentiality.

Level of action in the CPN: CNG level.

The main mechanism to perform Network Access Control is a firewall, i.e. a system designed to permit, deny or proxy data traffic to or from the customer's network. A firewall is positioned to control all incoming and outgoing traffic; hence the CNG is the perfect candidate to perform the firewall functions.

There are several approaches to implements firewall functionalities, such as:

- Packet Filtering: the simplest one inspects each incoming or outgoing IP packet permitting, dropping or rejecting it on the basis of simple policies (usually defined as access control list) such as the IP address and the protocol type.
- Stateful Firewall: in addition to a Packet Filter keeps track on IP packets belonging to the same connection thereby detecting whether a packet is part of an existing connection or a start of a new connection.
- Application Level Gateway: In addition to a stateful firewall can understand the behaviour of some applications and can detect e.g. if an illegal protocol is used for a given application or dynamically open ports for additional sessions belonging to a flow.

Firewalls can divide the network into subnets each one with a different level of security and different security policy as for example a demilitarized zone.

The firewall could have several configuration alternatives.

- A basic/minimum configuration to ensure a minimum level of security.
- One or several default configurations provided and managed by the operator/service provider through a remote management system.

- Additional alternative configurations that can depend on the user (e.g. there can be different configurations for parents and children). These user specific configuration could be managed by the same entity managing the user identity (e.g. the UICC).

6.4 Network Access Control (NAC)

The Network Access Control (NAC) is a gathering of methods linked to the control of a network's access. In term of security, these methods aim to control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. The combined tools used are usually enforced authentication, security policies for users, management of network resources, verification tools for security updates, and directory management.

6.4.1 Network Endpoint Assessment (NEA)

Security threats addressed:

- unauthorized access;
- breach of system/device integrity;
- breach of confidentiality.

Level of action in the CPN: CNG, CND.

Network Endpoint Assessment [4] architectures have been implemented in the industry in order to face the security threats of internal networks. The IETF NEA architectures have been defined to assess the "posture" of endpoint devices for the purposes of monitoring compliance to an organization's posture policy and optionally restricting access until the endpoint has been updated to satisfy the posture requirements. Posture refers to the hardware and software configuration of an endpoint and may include knowledge that software installed to protect the device (e.g. patches, anti-virus, firewall, host-based intrusion detection system or any custom software) is enabled and up-to-date.

In the CPN context, the NEA architecture could be used to allow only compliant and trusted Customer Network Devices (CND), such as PCs, IP-phone, and PDAs, onto the network, restricting or blocking the access (at the network layer) of noncompliant devices, and thereby limiting the potential damage from security threats and risks. Then NEA allows operators and service providers to enforce specific security policies on all CND as they enter the customer premises network, regardless of their access methods, ownership, device types, application configurations, etc.

The general NEA architecture is a client-server architecture, where the server component evaluates the posture of an endpoint device and provides network authorization decisions. Moreover the NEA server interacts with the NEA client (i.e. CND) by means of a specific software agent installed on each managed element. Usually such agents have a small footprint and low impact on the CND activities. In the CPN context, the Customer Network Gateway (CNG) is the natural candidate to perform the NEA server role.

6.5 Antispoofing

Security threats addressed:

- unauthorized access;
- initiation of unsolicited information;
- masquerade.

Level of action in the CPN: CNG level.

Spoofing is a technique consisting in using the IP address of a device in order to take over its identity. This technique allows the creation of IP packets with a source IP address belonging to someone else and can be used to tackle networks while being recognized as someone else and makes it possible to carry out DoS or unauthorized service access. Antispoofing functionality could help the protection of the NGN from attacks originated from the customer network.

Packet filtering is one defence against IP spoofing attacks. The gateway to a network usually performs ingress filtering, which is blocking of packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine. Ideally the gateway would also perform egress filtering on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing filtering from launching IP spoofing attacks against external machines.

It is also recommended to design network protocols and services so that they do not rely on the IP source address for authentication.

Some upper layer protocols provide their own defence against IP spoofing. For example, Transmission Control Protocol (TCP) uses sequence numbers negotiated with the remote machine to ensure that arriving packets are part of an established connection. Since the attacker normally can not see any reply packets, he has to guess the sequence number in order to hijack the connection. The poor implementation in many older operating systems and network devices, however, means that TCP sequence numbers can be predicted.

6.6 VPN capabilities

Security threats addressed:

- unauthorized access;
- breach of confidentiality;
- breach of system/device integrity.

Level of action in the CPN: CND-CNG, CNG-network, CND-network. A **Virtual Private Network** (VPN) is a communications network tunnelled through another network, and dedicated for a specific network. A VPN enables corporations or service providers to extend their services to employees and partners without the risk of compromising their integrity and confidentiality.

Different technologies (standard and proprietary solutions) can be adopted for VPN implementation such as encryption (IPSEC, Secure RTP (SRTP) to protect the payload, TLS, etc.) or traffic separation (e.g. MPLS).

Key management aspects have to be considered for further study.

6.6.1 VPN Capability Based on IPsec

IPsec can be used to create Virtual Private Networks (VPN), through its two different modes:

- transport mode (end-to-end).

Only the transferred data of the IP packet is encrypted and/or authenticated. The routing is intact (as the IP header is not modified/encrypted), but when the authentication header is used, the IP addresses cannot be translated. Transport mode is used for host-to-host communications.

- tunnel mode (portal-to-portal).

The entire IP packet (data plus the message headers) is encrypted and/or authenticated then encapsulated into a new IP packet for routing to work. Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.

NOTE: In IPv6 it is mandated to support IPsec but optional to deploy, and it is optional to deploy IPsec for use with IPv4.

Reference to "WLAN 3GPP IP Access" of TS 133 234 [5], i.e. scenario 3, may provide basis for this VPN functionality.

6.6.1.1 Remote access case

The payload traffic that goes between the CPN and a remote access device is not protected in the remote access service context. In TS 133 203 [6], IMS-AKA and IPsec together provide authentication and integrity protection but only for the signalling traffic between the CNG and NGN. With HTTP Digest only authentication protection is provided. Therefore, there is also a need of integrity and confidentiality protection for the payload traffic.

IPsec might be used to establish an encrypted communication channel between the CNG and a remote access device. IPsec provides both integrity and confidentiality protection for IP datagram according to RFC 1827 [12]. In addition IMS-AKA requires IPsec support in the Gm interface between UE and P-CSCF for integrity protection.

Remote access services that might benefit from such an encrypted communication channel include home surveillance, uploading content (files, photos or video clips) from a remote device to a home server and downloading content from a home server to a remote device.

6.6.2 Tunnelling using SSL/TLS

SSL/TLS used either for tunnelling the entire network stack, as in the OpenVPN project, or for securing what is, essentially, a web proxy. SSL is a framework more often associated with e-commerce, but it has been built-upon by a number of vendors to provide remote access VPN capabilities. A major practical advantage of an SSL-based VPN is that it can be accessed from the locations that restrict external access to SSL-based e-commerce websites only, thereby preventing VPN connectivity using IPsec protocols. SSL-based VPNs are vulnerable to trivial Denial of Service attacks mounted against their TCP connections because latter are inherently unauthenticated.

6.6.3 OpenVPN

OpenVPN is an open standard VPN. It is a variation of SSL-based VPN that is capable of running over UDP. Clients and servers are available for all major operating systems.

6.6.4 VPN Quarantine

The client machine at the end of a VPN could be a threat and a source of attack; this has no connection with VPN design and is usually left to system administration efforts. There are solutions that provide VPN Quarantine services which run end point checks on the remote client while the client is kept in a quarantine zone until healthy.

6.7 Anti-virus

Security threats addressed:

- breach of system/device integrity;
- initiation of unsolicited information;
- unauthorized access;
- breach of confidentiality;
- service availability.

Level of action in the CPN: CND, CNG.

Customer devices should be provided with an easy-to-use Anti-virus (AV) Engine to defend them from malicious code and viruses hidden inside files, e-mail or on the Web pages. Automatic real-time and off line scanning is essential to protect devices from potential threats that can occur for example during software download.

The CNG could be part of the anti-virus architecture, for example by taking into consideration the AV Relay function. An AV Relay has all the functionality to interact between the AV facility in the customer devices and the Security Operation Centre supplying the AV service. The AV Relay is able to synchronize the AV clients with the latest more updated AV signature file.

An AV engine can work with different detection methods, like:

Comparison with a known virus signature list. This list needs to be regularly updated, and stored in a secured way (e.g. in the UICC) to avoid any unauthorized access to modify it.

Various detection algorithms that can compare behaviours with usual or unusual viruses' behaviours, allowing detection of yet unknown viruses.

The CNG could also be equipped with an AV engine, in order to perform a real time scan of all the traffic passing through it. Considering strong implementation issues, this additional functionality can be considered only for non-residential scenarios, which is out of scope of the present document.

6.8 URL/URI filtering and prime user control

Security threats addressed:

- initiation of unsolicited information;
- unauthorized access.

Level of action in the CPN: CNG.

The possibility of denying a list of URLs/URIs or URLs/URIs that contain a specific pattern, to prevent another person from sending or receiving information (usually on the web) and mainly to restrict access to unsuitable/questionable material. This function is especially useful to implement parental control services directly inside the CNG.

6.9 Unsolicited communication prevention

Security threats addressed:

- breach of system/device integrity;
- initiation of unsolicited information;
- unauthorized access.

Level of action in the CPN: CNG, CND.

Unsolicited Communication (UC) can apply on different types of communication in the NGN:

- Bulk (recorded) text messages (aka SPAM).
- Bulk (recorded) other multimedia messages (aka SPIT).
- More advanced attack scenarios (can be found in the WI07025).

As defined in TR 187 009 [17] the NGN should provide the ability of identifying and preventing UC in the network. This can be done in a two step approach:

1) Detection and marking in a system wide approach (i.e. global blacklist, call-rate analysis, etc.).
2) Detection and handling in a personalized way (i.e. redirect to Junk-mail or decline call).

Only the second step is in the scope of this WI where a user should be able to directly interact with a UC prevention system at his premises (e.g. the CNG). This UC prevention entity should be able to filter in a personalized way the UC attempts (i.e. by personalized blacklists, call-rate or more advanced filtering) and may even handle/prevent UC attempts by e.g. redirect to Junk-mail or decline call). This UC Prevention Entity should also interpret system-wide (step 1 clause 6.9) marking of calls, if such a system is implemented.

The advantage of this approach would be that the user has direct control over the UC rating and handling, and final responsibility for call acceptance/rejection remains ultimately with the user (and not the operator).

For more information please go to TR 187 009 [17] (Feasibility study of prevention of unsolicited communication in the NGN).

NOTE: Further information on Unsolicited Communication Prevention is provided in 3GPP SA3 Technical Report on anti-SPAM solutions for SMS, MMS and IMS.

There are some open issues on the location of black lists (CNG, CND, network), the marking functionalities.

6.10 Intrusion detection system

Security threats addressed:

- breach of system/device integrity;
- initiation of unsolicited information;
- unauthorized access;
- breach of confidentiality.

Level of action in the CPN: CNG.

An Intrusion Detection System (IDS) monitors data traffic inside a network segment in order to reveal malicious traffic. It complements a firewall by introducing more thorough inspection mechanisms than a firewall. Typically an IDS is able to detect protocol anomalies, malicious traffic patterns etc. More advanced systems are called Intrusion Prevention Systems that can also drop traffic that is violating the security policy and Unified Threat Management (UTM) Systems that can also perform anti-virus operation and spam filtering.

IDS monitors network traffic for suspicious activity alerting the network administrator of possible security problems. IDS system should be placed at strategic points inside the network to monitor traffic to and from all devices in the network, such as the border between the private, secure, LAN and the public insecure network (Internet) where the IDS system can scan all inbound and outbound traffic. In this sense the Customer Network Gateway would be a suitable location for the IDS function.

The most suitable IDS technology for the customer environment is the "signature based" one, where the system monitors packets on the network and compares them against a database of signatures taken from known malicious threats. Hence it is very important that the database of signatures is always up to date.

In case of tentative intrusion, there can be the need of alerting a particular entity. Alerts and actions can be configurable.

Strong implementations issues at the CNG level have to be considered.

6.11 Network Address Translation (NAT)

Network Address Translation (NAT) is not a security mechanism but may be used in combination with security mechanisms. TR 187 008 [11] addresses NAT traversal issue.

7 Recommendations for security mechanisms implementation

7.1 Authentication and authorization mechanisms

The support for user/entity authentication and authorization functionality is proposed as **recommended** in the CNG.

For all the various authentication needs, the UICC could be used if available.

7.1.1 Wireless security mechanisms

The support for wireless security functionalities are proposed as **recommended** in the CNG.

The support for wireless security functionalities are proposed as **recommended** in the CND.

7.2 Security Management functionality

This functionality is proposed as **recommended** in the CNG.

7.3 Firewall

This functionality is proposed as **recommended** in the CNG.

For the mean of storing the various possible additional firewall configurations (in relation to the basic default one provided by the CNG), it could be considered to store these configuration in the UICC if available. This would allow the Network Access Providers to update securely their own configuration parameters, and the end user to be able to move his/her personal configuration from one CNG to another (e.g. in case of change of the CNG).

7.4 Network Access Control

7.4.1 Network Endpoint Assessment

The support for Network Endpoint Assessment (NEA) functionality is proposed as **optional** in the CNG.

The support for Network Endpoint Assessment (NEA) functionality is proposed as **optional** in the CND.

7.5 Antispoofing

This functionality is proposed as **recommended** in the CNG.

7.6 VPN capabilities

This functionality is proposed as optional in the CNG.

If available the UICC should be used to provide the pre-requisite for the tunnel creation (e.g. the shared secret keys, the signature elements, etc.).

7.7 Anti-virus

This functionality is proposed as optional in the CNG.

7.8 URL/URI filtering and prime user control

This functionality is proposed as **optional** in the CNG.

NOTE: In the internet world, more and more governments are requesting the ISP to provide such a feature.

It can be considered to store the user control data in the UICC if available. This would allow the subscription owner to be able to move his/her personal configuration from one CNG to another (e.g. in case of change of the CNG).

7.9 Unsolicited communication prevention

This functionality is proposed as optional in the CNG.

This functionality is proposed as optional in the CND.

7.10 Intrusion detection System

This functionality is proposed as optional in the CNG.

7.11 Network Address Translation

This functionality is proposed as **recommended** in the CNG.

7.12 Summary

7.12.1 CNG

Summary table for CNG:

Mechanisms	CNG
Authentication and authorization	Recommended
Security Management functionality	Recommended
Firewalling	Recommended
Network Access Control	Optional
Antispoofing	Recommended
VPN capabilities	Optional
Anti-virus	Optional
URL/URI filtering and prime user control	Optional
Unsolicited communication prevention	Optional
Intrusion detection System	Optional
NAT	Recommended

7.12.2 CND

Security Management functionality and authentication mechanisms are mandatory for the CND in general. For the others mechanisms, it is up to the manufacturers and the operators to decide whether to implement them.

History

Document history		
V2.0.0	February 2008	Publication