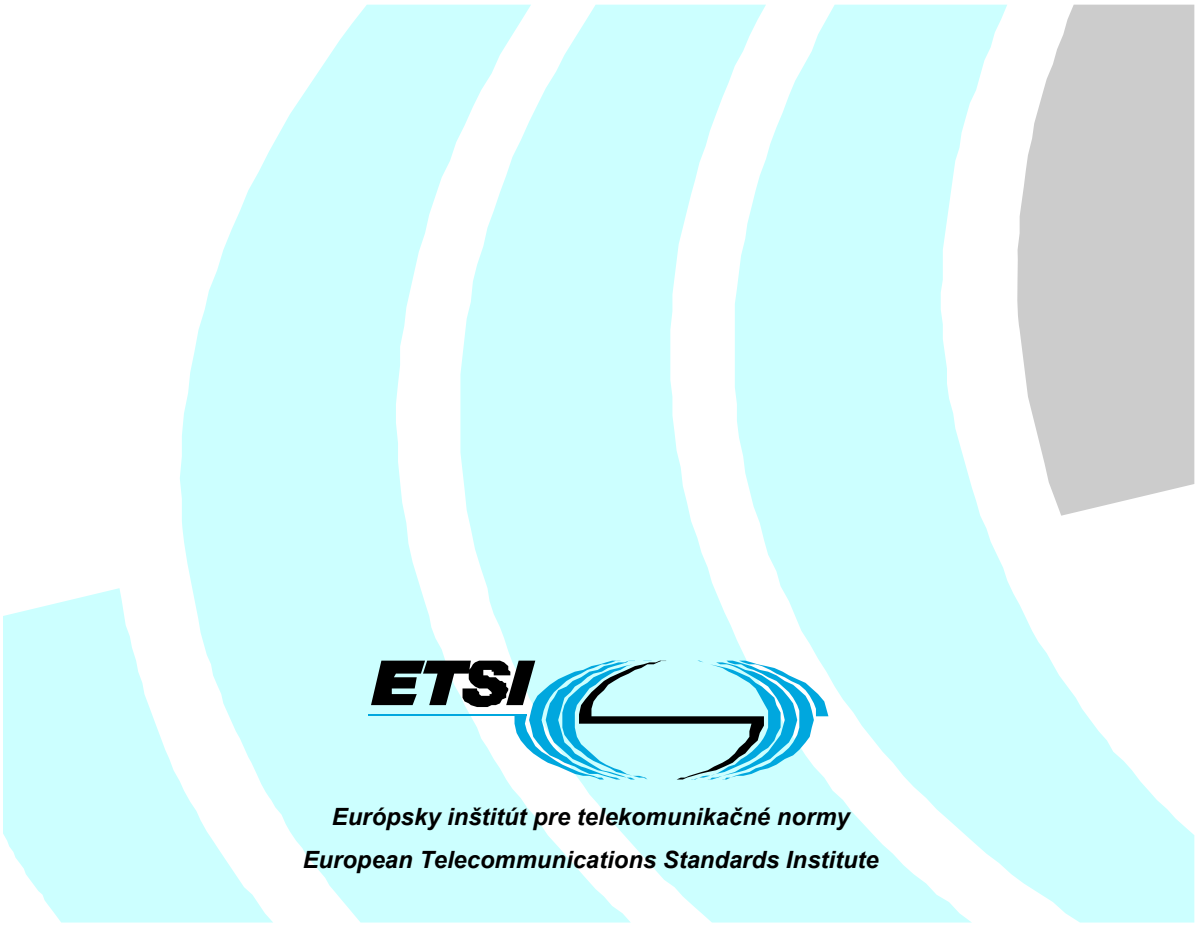
ETSI TS 187 001 V2.1.5 (2008-10)

Technická špecifikácia

Telekomunikačné a internetové konvergované služby a protokoly na zdokonalené siete (TISPAN; Bezpečnosť NGN (SEC) Požiadavky

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocols for Advanced Networking (TISPAN). NGN SECurity (SEC) Requirements



Európsky inštitút pre telekomunikačné normy

European Telecommunications Standards Institute

Referenčné číslo

RTS/TISPAN-07026-NGN-R2

Deskriptory

security, service

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

Neziskové združenie registrované
na podprefektúre de Grasse (06) N° 7803/88

Dôležité upozornenie

Jednotlivé kópie tohto dokumentu možno stiahnuť zo stránky:

http://pda.etsi.org/

Tento dokument môže byť dostupný vo viacerých elektronických verziách alebo v tlačenej forme. V prípade existujúceho alebo viditeľného rozdielu v obsahu medzi takýmito verziami je referenčnou verziou verzia v prenosnom dokumentovom formáte (Portable Document Format – PDF).

V prípade sporu je referenčným výtlačok vytlačený na tlačiarni ETSI z verzie PDF uchovávanej na určenom sieťovom serveri sekretariátu ETSI.

Používatelia tohto dokumentu by mali brať do úvahy, že dokument môže byť revidovaný alebo sa môže zmeniť jeho postavenie. Informácie o postavení tohto dokumentu a ďalších dokumentov ETSI sú dostupné na http://portal.etsi.org/tb/status/status.asp

Ak nájdete v tomto dokumente chyby, svoje pripomienky zašlite na:

http://portal.etsi.org/chaircor/ETSI_support.asp

Oznam o autorských právach

Obsah

Práva duševného vlastníctva

Práva duševného vlastníctva, ktoré majú alebo môžu mať zásadný význam pre tento dokument, mohli sa oznámiť organizácii ETSI. Informácie o týchto zásadných právach duševného vlastníctva, ak existujú, sú **pre členov i nečlenov** ETSI verejne dostupné a môžu ich nájsť v dokumente ETSI SR 000 314 s názvom *Práva duševného vlastníctva (IPR). Zásadné alebo potenciálne zásadné práva duševného vlastníctva oznámené organizácii ETSI vo vzťahu k normám ETSI,* ktorý možno získať na sekretariáte ETSI. Najnovšie znenie je dostupné na serveri ETSI (http://webapp.etsi.org/ipr).

V súlade so svojou politikou v oblasti práv duševného vlastníctva ETSI neskúma ani nevyhľadáva nijaké práva duševného vlastníctva. Neposkytuje ani záruku na iné práva duševného vlastníctva, ktoré sa neuvádzajú v dokumente SR 000 314 (alebo v jeho aktualizovaných vydaniach na serveri ETSI), ktoré sú alebo môžu byť, alebo by sa mohli stať dôležitými pre predkladaný dokument.

Predhovor

Technickú špecifikáciu (TS) vypracovala technická komisia ETSI Telekomunikačné a internetové konvergované služby a protokoly na zdokonalené siete (TISPAN).

Úvod

V technickej špecifikácii sa definujú požiadavky na bezpečnosť TISPAN NGN R1, zatiaľ čo stav architektúry a prehľad 2. implementácie sú obsiahnuté v architektúre bezpečnosti R1 (TS 187 003 [1]).

1 Predmet

V technickej špecifikácii sa definujú požiadavky na bezpečnosť NGN verzia 2 podľa TISPAN. V tejto technickej špecifikácii sa uvádzajú požiadavky na rozličné podsystémy NGN definované v 1. stupeň. V tejto technickej špecifikácii sa uvádzajú požiadavky na bezpečnosť na chrbticovú sieť NGN a prístupovú sieť NGN.

Hlavnou úlohou požiadaviek na bezpečnosť rozličných podsystémov je určiť požiadavku v týchto hlavných oblastiach:

- bezpečnostnú stratégiu;
- overovanie totožnosti, autorizáciu, kontrolu prístupu a zber údajov – účtovanie;
- identifikáciu a bezpečnú registráciu;
- požiadavky na komunikáciu a dátovú bezpečnosť (vrátane stavu dôveryhodnosti, integrity);
- súkromie;
- riadenie kľúčov;
- spoluprácu NAT/fireval;
- dostupnosť a ochranu pred DoS;
- zabezpečenie;
- stupeň bezpečnostných mechanizmov.

2 Referenčné dokumenty

Odkazy sú špecifikované (určené dátumom vydania, číslom vydania, číslom verzie atď.), alebo nešpecifikované.

- V prípade špecifikovaného odkazu neplatia ďalšie revízie.
- Nešpecifikovaný odkaz sa môže vytvoriť len na úplný dokument alebo na jeho časť a len v týchto prípadoch:
  - ak sa akceptuje, že to bude možné použiť na všetky budúce zmeny v dokumente na účely odkazu na dokument;
  - na informatívne odkazy.

Uvádzané dokumenty, ktoré nie sú verejne dostupné v očakávanom mieste, môžu sa vyhľadať na http://docbox.etsi.org/Reference.

V odkaze na dokumenty s priamym prístupom sa musia poskytnúť informácie dostatočné na identifikáciu a umiestnenie zdroja. Na zaistenie vyhľadávania sa uprednostňuje, aby sa citoval primárny zdroj odkazu na dokument. Odkaz musí, ak sa dá, zostať platný počas očakávanej životnosti dokumentu. Odkaz musí obsahovať spôsob prístupu k dokumentu a úplnú sieťovú adresu s rovnakou interpunkciou a použitím písmen s hornými a dolnými indexmi.

> POZNÁMKA. – Pokiaľ akýkoľvek hyperlink obsiahnutý v tejto kapitole bol platný v čase publikovania, ETSI nemôže garantovať jeho platnosť z dlhodobého hľadiska.

2.1 Normatívne referenčné dokumenty

Na špecifikáciu sú uvedené dokumenty nevyhnutné. Pri datovaných odkazoch sa použijú len citované vydania. Pri nešpecifikovaných odkazoch, sa použije posledné vydanie dokumentu (vrátane akýchkoľvek dodatkov).

[1] Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). NGN Security. Security Architecture

[2] Digital cellular telecommunications system (Phase 2+). Universal Mobile Telecommunications System (UMTS). 3G security. Access security for IP-based services (3GPP TS 33.203)

[3] Digital cellular telecommunications system (Phase 2+). Universal Mobile Telecommunications System (UMTS). 3G security. Network Domain Security (NDS). IP network layer security (3GPP TS 33.210)

[4] Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON). Evaluation criteria for cryptographic algorithms

2.2 Informatívne referenčné dokumenty

Ďalej uvedené dokumenty nie sú dôležité v tejto technickej špecifikácii, ale pomáhajú používateľovi v konkrétnej predmetnej oblasti. Pri nešpecifikovaných odkazoch sa použije posledné vydanie dokumentu (vrátane akýchkoľvek dodatkov).

[i.1] ISO 15408-1 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[i.2] IEEE 802.1X Port Based Network Access Control

[i.3] ISO 15408-2 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components

[i.4] IETF RFC 3324 Short Term Requirements for Network Asserted Identity

[i.5] IETF RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[i.6] ETSI ES 283 002: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) – H.248 Profile for controlling Access and Residential Gateways

[i.7] ETSI TS 187 005 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) – NGN Lawful Interception – Lawful interception functional entities, information flow and reference points

[i.8] ETSI TS 133 310 Universal Mobile Telecommunications System (UMTS) – Network domain security – Authentication framework (NDS/AF) (3GPP TS 33.310)

[i.9] ETSI TS 133 234 Universal Mobile Telecommunications System (UMTS) – 3G security – Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)

[i.10] ISO 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[i.11] ETSI TR 187 011 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) – NGN Security – Application of ISO 15408-2 requirements to ETSI standards – guide, method and application with examples

[i.12] ETSI TR 187 010 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) – NGN Security – Report on issues related to security in identity imanagement and their resolution in the NGN

[i.13] ETSI TS 124 229 Digital cellular telecommunications system (Phase 2+) – Universal Mobile Telecommunications System (UMTS) – Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 (3GPP TS 24.229)

3 Termíny, definície a skratky

3.1 Termíny a definície

V dokumente sa používajú termíny a definície:

anonymná komunikácia (angl. **anonymous communication)**: komunikácia, pri ktorej používateľ prijímajúci komunikačnú reláciu nemôže identifikovať volajúceho používateľa

zabezpečený kanál (angl. **trusted channel)**: prostriedky, ktorými NGN a vzdialená NGN/NGCN môžu komunikovať s potrebnou dôvernosťou podporujúcou stratégiu bezpečnosti NGN (podľa normy ISO 15408-1 [i.1])

zabezpečená trasa (angl. **trusted path):** prostriedky, ktorými používateľ a NGN/NGCN môžu komunikovať s potrebnou dôvernosťou podporujúcou stratégiu bezpečnosti NGN (podľa normy ISO 15408-1 [i.1])

zabezpečená doména (angl**. trusted domain):** v súvislosti s jednou alebo viacerými NGN prepojenými v NNI podľa definície uvedenej v čl. 4.4 TS 124 229 zabezpečenie, ktoré sa dosiahne implementáciou jedného alebo viacerých bezpečnostných mechanizmov definovaných v TS 187 003 [1]

3.2 Skratky

V dokumente sa používajú skratky:

3G	3rd Generation	tretia generácia
3GPP	3rd Generation Partnership Project	projekt partnerstva tretej generácie
AA	Authentication & Authorization	overovanie totožnosti a autorizácia
ACR	Anonymous Communications Rejection	odmietnutie anonymnej komunikácie
AF	Application Function	aplikačná funkcia
AGW	Access Gateway	prístupový sieťový priechod
ALG	Application Layer Gateway	sieťový priechod aplikačnej vrstvy
AP	Authentication Proxy	zástupný server autentifikácie
AS	Application Server	aplikačný server
CNG	Customer Network Gateway	účastnícky sieťový priechod
CPE	Customer Premises Equipment	zariadenie v priestoroch zákazníka
CPN	Customer Premises Network	sieť v priestoroch zákazníka
CSCF	Call Session Control Function	funkcia riadenia relácie volania
DoS	Denial-of-Service	vyradenie služby
EAP-AKA	Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement	metóda rozšírenia protokolu autentifikácie v UMTS a dohoda o kľúčovaní a autentifikácii
HSS	Home Subscriber Server	domáci účastnícky server
ID	IDentity	identita
IKE	Internet Key Exchange	internetová výmena kľúčov
IMPU	IMS PUblic user ID	ID verejného používateľa IMS
IMS	IP multimedia Subsystem	multimediálny subsystém IP
IP	Internet Protocol	internetový protokol
ISIM	IMS Subscriber Identity Module	účastnícky identifikačný modul IMS
IT	Information Technology	informačná technika
MAC	Message Authentication Code	kód overenia správy
MD	Message Digest	roztriedenie správy
NAF	operator controlled Network Application Function	sieťová aplikačná funkcia riadená prevádzkovateľom
NASS	Network Access SubSystem	subsystém prístupu k sieti
NAT	Network Address Translation	prevod sieťových adries
NDS	Network Domain Security	bezpečnosť sieťovej domény
NGCN	Next Generation Corporate Network	podniková sieť novej generácie
NGN	Next Generation Network	sieť novej generácie
NICC	Network Interoperability Consultative Committee	konzultačný výbor na sieťovú interoperabilitu
PAI	Public Administration International	medzinárodná verejná správa
P-CSCF	Proxy - Call Session Control Function	riadiaca funkcia sprostredkovania volania
PES	PSTN/ISDN Emulation Subsystem	subsystém emulácie PSTN/ISDN
RACS	Resource Admission Control Subsystem	subsystém riadenia prostriedku a vstupnej kontroly
RGW	Residential Gateway	bytový sieťový priechod
S-CSCF	Serving - Call Session Control Function	riadiaca funkcia obsluhujúceho servera volania
SEGF	SEcurity Gateway Functions	funkcie bezpečnostného sieťového priechodu

SF	Security Functions	bezpečnostné funkcie
SIP	Session Initiation Protocol	protokol inicializácie relácie
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking	telekomunikačné a internetové konvergované služby a protokoly na zdokonalené siete
TOE	Target of Evaluation	cieľ hodnotenia
TS	Technical Specification	technická špecifikácia
UAS	User Agent Server	server používateľského agenta
UE	User Equipment	zariadenie používateľa
UICC	Universal Integrated Circuit Card	univerzálna karta s integrovaným obvodom
UMTS	Universal Mobile Telecommunication System	univerzálny mobilný telekomunikačný systém

4 Požiadavky na bezpečnosť

Požiadavky na bezpečnosť opísané v kapitole4 sú pre skrátené odvolávanie označené symbolickým identifikátorom požiadavky na bezpečnosť (napríklad R-SP-n) spolu s určitým textovým opisom. Požiadavky na bezpečnosť sú zaradené do zoznamu bez akejkoľvek predpokladanej dôležitosti alebo priority. Je poukázané, že nie všetky požiadavky na bezpečnosť sa vzájomne nevylučujú, ale skutočne medzi nimi existuje určité neželateľné prekrytie.

Vysoko postavené ciele

NGN musí podporiť bezpečné a dôveryhodné prostredie pre účastníkov, prevádzkovateľov siete a poskytovateľov služby na splnenie súboru komplexných a základných požiadaviek na bezpečnosť.

Bezpečnostné ciele určené služobnými požiadavkami zamedzujú maskovanie, DoS, manipuláciu dát, podvod a zneužívanie siete, poškodzovanie jednej časti siete prepojením s menej bezpečným prostredím.

ISIM sa musia umiestniť na UICC. Použitie ISIM na UICC je preferované riešenie na dosiahnutie požiadaviek na bezpečnosť na prístup k funkciám IMS v NGN. Nepredpokladajú sa existujúce riešenia, ako napríklad roztriedenie overenia totožnosti na umožnenie včasných právnych implementácií. ISIM sa môže umiestniť v samotnom zariadení alebo prístupný diaľkovo cez miestne rozhranie k zariadeniu s UICC.

Požiadavky na bezpečnosť pre používateľov, poskytovateľov služby (prístup, aplikácia) sa môžu meniť. Bezpečnostná architektúra NGN nesmie sa obmedziť na jednu bezpečnostnú stratégiu. Každá bezpečnostná služba (overovanie totožnosti, integrita dát, opakované detegovanie, dôvernosť) musí sa použiť nezávisle od iných, len ak je to možné. Výber služieb sa má zakladať na stratégii.

Bezpečnostné mechanizmy nezavádzajú nové útoky DoS. Niektoré bezpečnostné mechanizmy a algoritmy požadujú značné spracovanie alebo ukladanie, v takom prípade bezpečnostné protokoly by mali chrániť seba, ak je to možné, proti záplavovým útokom, ktoré zaplavia koncový bod spracovania alebo ukladania. Splnenie požiadaviek na predpokladanú vysokú dostupnosť bude schopné zmierniť útoky na vyradenie služby.

4.1 Požiadavky na bezpečnostnú stratégiu

Bezpečnostná stratégia definuje legitímnych používateľov systému a čo im je umožnené robiť. Určí sa, aké informácie sa musia chrániť od akých ohrození. V prostredí s heterogénnou spoločnosťou používateľov, so zariadeniami od viacerých dodávateľov, s rozličnými modelmi ohrozenia a nepravidelným rozmiestnením funkčnej bezpečnosti zabezpečiť, aby bezpečnosť bola správne funkčná, je mimoriadne ťažké bez vykonateľnej stratégie.

(R-SP- 1) – Sieť NGN v TISPAN sa musí logicky a fyzicky rozdeliť na bezpečnostné domény umožňujúce oddelenie aplikácie (napríklad IMS) a prenosu (napríklad ADSL alebo UMTS). Rozliční prevádzkovatelia podobných sietí (napríklad IMS) musia byť schopní prevádzkovať svoje vlastné bezpečnostné stratégie.

(R-SP- 2) – Bezpečnostné mechanizmy a iné parametre prednastavené mechanizmami bezpečnosti sa musia konfigurovať. To musí byť stabilné na rozhraní NNI a môže sa to dohodnúť na rozhraniach UNI. Dohodnutie bezpečnostného mechanizmu musí mať definovanú určitú minimálnu úroveň podľa

bezpečnostnej domény, napríklad zamedziť útoky na vyradenie ponuky (bidding-down). Používatelia musia byť schopní odmietnuť komunikáciu, ktorá nespĺňa ich minimálnu bezpečnostnú stratégiu.

(R-SP- 3) – Bezpečnostný mechanizmus sa musí rozdeliť tak, aby funkcie overenia totožnosti, dátovej integrity, opakovania detegovania a dôvernosti mohli sa implementovať a vybrať navzájom nezávisle podľa významu.

(R-SP- 4) – UE vždy ponúka šifrovací algoritmus na P-CSCF na použitie v relácii a stratégia P-CSCF musí definovať, či použije, alebo nepoužije šifrovanie.

(R-SP- 5) – UE a P-CSCF si musia dohodnúť algoritmus integrity, ktorý sa musí použiť v relácii.

(R-SP- 6) – Stratégia HN sa musí použiť na rozhodnutie, ak sa musí brať do úvahy overovanie totožnosti na registráciu rozličných IMPU, napríklad patriacich k rovnakým alebo odlišným profilom služby.

(R-SP- 7) – Funkcie bezpečnostného sieťového priechodu (SEGF) musia zodpovedať za uskutočnenie bezpečnostných stratégií pre spoluprácu medzi sieťami.

POZNÁMKA. – Aktuálna medzidoménová bezpečnostná stratégia nie je štandardizovaná a je ponechaná na voľné uváženie v roamingových dohodách prevádzkovateľov.

(R-SP- 8) – SEGF sú zodpovedné za bezpečnosť chúlostivých činností a musia ponúkať schopnosti na bezpečné uloženie kľúčov z dlhodobého hľadiska použitých na overovanie totožnosti IKE.

4.2 Požiadavky na overovanie totožnosti, autorizáciu, kontrolu prístupu a zber údajov na účtovanie

Všeobecný autentický prístup

(R-AA-1) – Prístup k sieťam, službám a aplikáciám NGN sa umožní len autorizovaným používateľom.

(R-AA- 2) – Overovanie totožnosti IMS v NGN R1 a R2 musí podporovať staršie rozšírené varianty (podporované používanými zariadeniami), hoci rozširovanie takýchto variantov sa ponecháva na prevádzkovateľov.

(R-AA- 3) – V iných ako starších rozšírených variantoch, overovanie totožnosti IMS musí byť nezávislé od overenia totožnosti na prístupe.

(R-AA- 4) – ISIM sa musí použiť na prístup k akejkoľvek službe IMS, hoci výnimky sa môžu povoliť pri tiesňovom volaní a starších rozšírených variantoch.

(R-AA- 5) – Overovanie totožnosti z ISIM medzi účastníkom IMS a sieťou musí spĺňať časť overenia totožnosti podľa bezpečnosti prístupu na služby IP uvedené v TS 133 203 [2].

(R-AA- 6) – Opakované overovanie totožnosti z ISIM účastníka IMS musí spĺňať časť overenia totožnosti podľa bezpečnosti prístupu na služby IP uvedené v TS 133 203 [2].

(R-AA- 7) – Musí sa zabrániť použitiu určitého ISIM k prístupu k sieťam a službám NGN a má sa to dať zrušiť pri konkrétnom ISIM.

(R-AA- 8) – Dôležité špecifické informácie ISIM v NGN sa musia chrániť pred neoprávneným prístupom alebo zmenou.

(R-AA- 9) – Overovanie totožnosti používateľa môže byť hardvérové (UE v 3GPPP: ISIM, napríklad skúškou fyzického znamienka) alebo softvérové (napríklad skúškou poznania určitých utajených informácií).

Staršie rozmiestnenie

(R-AA- 10) – Musí sa podporovať overovanie totožnosti používateľa – IMS v NGN mechanizmami SIP Digest, čo je starší rozšírený variant.

(R-AA- 11) – Ak prevádzkovatelia IMS v NGN využívajú riešenia Digest a ISIM, potom prevádzkovateľ musí určiť mechanizmus overenia totožnosti (SIP Digest alebo ISIM) pre každého konkrétneho používateľa. Mechanizmus overenia totožnosti sa musí využívať podľa informácie o predplatnom v profile používateľskej služby a špecifickej stratégie prevádzkovateľa IMS v NGN. Ak koncové zariadenie podporuje riešenie ISIM a prevádzkovateľ siete podporuje aj ISIM, aj staršie rozvojové riešenie, musí sa použiť riešenie ISIM.

(R-AA- 12) – Prenášané heslá sa musia dostatočne chrániť, napríklad šifrovaním alebo iným spôsobom.

(R-AA- 13) – V špeciálnych začiatočne využívaných variantoch (pozri poznámku 1), ak overovanie totožnosti IMS je spojené s overením totožnosti na prístupe, musí sa umožniť získanie prístupu k službám IMS po procedúre overenia totožnosti. Overovanie totožnosti poskytne súčasný prístup k sieti a službám IMS.

POZNÁMKA 1. – Existujú dva špeciálne začiatočne využívané varianty (takisto súvisia s overením totožnosti NASS Bundled):
(A) – Overovanie totožnosti IMS je spojené s overením totožnosti prístupového spoja (nie je putovanie).
(B). – Overovanie totožnosti IMS je spojené s overením totožnosti prístupu s konektivitou IP (obmedzené putovanie sa môže poskytovať).

POZNÁMKA 2. – Overovanie totožnosti na prístupe môže spôsobiť v službách IMS zviazanie k prístupovému bodu (spoju) alebo k poslednému spojeniu IP (zariadeniu). V druhom prípade môže byť dostupné obmedzené putovanie. Na získanie prístupu k službám IMS sa nepožaduje špecifické overovanie totožnosti IMS z CPE/koncového zariadenia.

(R-AA- 14) – Podsystém NGN musí mať schopnosť definovať a vykonávať stratégiu vzhľadom na schválenie overenia totožnosti používateľa.

Rozhranie Ut

(R-AA- 15) – Medzi UE a AS sa pred poskytnutím oprávnenia musí podporovať vzájomné overovanie totožnosti.

(R-AA- 16) – Má sa umožniť podpora architektúry založenej na overovacom serveri.

POZNÁMKA 1. – Účelom AP je oddeliť procedúru overenia totožnosti a logiku špecifickej aplikácie AS na rozličné logické jednotky.

(R-AA- 17) – Medzi UE a AP sa musí podporovať vzájomné overovanie totožnosti.

(R-AA- 18) – AP musí rozhodnúť, či konkrétny účastník (napríklad UE), je oprávnený na prístup ku konkrétnemu AS.

(R-AA- 19) – Ak sa použije AP, AS musí len autorizovať požiadavku na prístup k požadovanému prostriedku.

POZNÁMKA 2. – AS nepotrebuje výslovne overiť totožnosť používateľa.

NASS

(R-AA- 20) – Medzi CPE a NASS sa musí podporovať vzájomné overovanie totožnosti počas registrácie úrovne prístupovej siete.

(R-AA- 21) – Prístupová sieť musí byť schopná overiť totožnosť a autorizovať prístup účastníka.

(R-AA- 22) – Overovanie totožnosti a autorizáciu k prístupovej sieti kontroluje prevádzkovateľ prístupovej siete.

(R-AA- 23) – Atribúty požadované na overovanie totožnosti používateľa prístupovou sieťou môže poskytovať prevádzkovateľ siete, u ktorého má používateľ IMS v NGN predplatné.

(R-AA- 24) – NASS musí podporovať použitie explicitného (napríklad PPP alebo IEEE 802.1x [i.2]) alebo implicitného spôsobu overenia totožnosti (napríklad overovanie totožnosti adresy MAC alebo overovanie totožnosti spoja) používateľmi/účastníkmi. V prípade implicitného overenia totožnosti sa musí spoliehať len na implicitné overovanie totožnosti fyzickej alebo logickej identifikácie na transportnej vrstve L2 (vrstva 2).

(R-AA- 25) – V prípade, ak CNG je smerovací modem a sieť na strane účastníka (CPN) v privátnej oblasti IP, overovanie totožnosti sa musí inicializovať z CNG.

(R-AA- 26) – V prípade, ak CNG je mostík, každé UE musí overiť totožnosť s NASS, ak oblasť IP v CPN rozpozná prístupová sieť.

RACS

R-AA- 27) – RACS a AF si musia vzájomne overiť totožnosť pred autorizáciou prostriedku.

(R-AA- 27A) – AF a SPDF v RACS musia byť schopné sa vzájomne identifikovať, ak vykonávajú overovanie totožnosti.

Iné špecifické požiadavky

(R-AA- 27) – Kontrolér mediálneho sieťového priechodu musí byť schopný spracovať overovanie totožnosti viacerých mediálnych sieťových priechodov, napríklad udržať viacnásobné bezpečnostné spojenia k rozličným mediálnym sieťovým priechodom.

(R-AA- 28) – Overovanie totožnosti používateľov NGN a overovanie totožnosti koncových zariadení NGN musia byť oddelené.

(R-AA- 29) – Identifikácia volajúceho a informácia o lokalite sa musia uložiť podľa všeobecného európskeho regulačného rámca poskytovateľom služby EMTEL. Identifikáciu volajúceho a informáciu o lokalite musí potvrdiť poskytovateľ služby EMTEL.

4.3 Požiadavky na identifikáciu a bezpečnú registráciu

Nasledujúce požiadavky sa snažia znížiť maskovanie, parodovanie a falošnú prezentáciu koncových zariadení NGN, zariadení/systémov (HW/SW) a používateľov. Požiadavky sa

snažia poskytnúť opatrenia proti krádeži identifikácie, chybnému/autorizovanému použitiu služieb/aplikácií NGN.

(R-IR- 1) – Musí sa umožniť implicitná registrácia IMPU. Všetky implicitne registrované IMPU patria k rovnakému profilu služby. Všetky implicitne registrovateľné IMPU musia doručiť HSS k S-CSCF a následne k P-CSCF. S-CSCF musí posudzovať všetky implicitne registrované IMPU ako registrované IMPU.

(R-IR- 2) – Identifikácia prístupu sa musí použiť na overovanie totožnosti prístupu. Táto identifikácia sa môže, ale nemusí použiť na iné účely.

(R-IR- 3) – Identifikácia ID sa musí dať použiť na overovanie totožnosti spoja.

4.4 Požiadavky na komunikáciu a dátovú bezpečnosť

Článok 4.4 obsahuje také požiadavky, ktoré určujú bezpečnosť komunikácie a dát. Dáta v tejto súvislosti môžu predstavovať používateľské dáta (napríklad hlas, video, textový tok) alebo riadiace dáta.

4.4.1 Všeobecné požiadavky na komunikáciu a dátovú bezpečnosť

Všeobecne

(R-CD-1) – Dôvernosť a integrita signalizácie IMS sa musia použiť spôsobom od uzla k uzlu (UE k P-CSCF a medzi inými NE).

NDS

(R-CD- 2) – Bezpečnostná sieťová doména (NDS) sa musí poskytovať na sieťovej vrstve a musí spĺňať požiadavky uvedené v TS 133 210 [3].

(R-CD- 3) – Celá prevádzka NDS/IP musí prejsť cez SEGF (funkcia bezpečnostného sieťového priechodu) pred vstupom do bezpečnostnej domény alebo pred jej opustením. Prevádzkovateľ IMS musí prevádzkovať rozhranie Za NDS/IP medzi SEGF podľa TS 133 210 [3].

(R-CD- 4) – V sieťovej doméne sa musí poskytovať bezpečnosť na rozhraní Cx.

Bezpečnosť prístupu

(R-CD- 5) – Bezpečný prístup IMS musí podporovať riešenie založené na ISIM (overovanie totožnosti, dôvernosť a ochranu integrity) na signalizáciu k používateľovi a od používateľa.

(R-CD- 6) – Medzi UE a P-CSCF sa musí poskytovať bezpečný spoj na ochranu v referenčnom bode Gm.

(R-CD- 7) – Prípad overenia totožnosti prístupu je nezávislý od overenia totožnosti IMS.

- Riešenie prístupu k chrbticovej sieti NGN musí poskytovať bezpečný prenos signalizácie k chrbticovej sieti NGN nezávisle od prístupovej technológie.

- Riešenie prístupu k chrbticovej sieti NGN musí poskytovať bezpečný prenos signalizácie k chrbticovej sieti NGN nezávisle od prítomnosti medziľahlých sietí IP pripájajúcich prístup NGN s chrbticovou sieťou NGN.

- Riešenie na prístup k chrbticovej sieti NGN musí umožniť vzájomné overovanie totožnosti koncového používateľa a chrbticovej siete NGN. Koncové zariadenie musí overiť totožnosť používateľa.

(R-CD- 8) – V prípade, kde overovanie totožnosti je spojené s overením totožnosti prístupového spoja, základná prístupová technológia musí poskytovať ochranu signalizácie a používateľských dát NGN.

(R-CD- 9) – Špecifická informácia ISIM sa musí aktualizovať bezpečným spôsobom.

Ut

(R-CD-10) – Musí sa umožniť ochrana dôverných dát (ako informáciu o prítomnosti a oprávnenia) pred útokmi (napríklad pred odpočúvaním, narušením a opakovanými útokmi).

RACS

(R-CD-11) – Nedefinované.

Iné špecifické požiadavky

(R-CD-12) – Všetky dáta súvisiace s konfiguráciou UE v referenčnom bode e3 sa musia zabezpečiť pred stratou dôvernosti a stratou integrity.

4.4.2 Požiadavky na integritu a ochranu pred prehrávaním

Všeobecne

(R-CD- 13) – Musí sa poskytovať ochrana integrity signalizácie, kontrola komunikácie a uložených dát.

(R-CD- 14) – Musí sa zaistiť pôvod, integrita a obnova dát overenia totožnosti, osobitne šifrovacieho kľúča.

Bezpečnosť prístupu

(R-CD- 15) – Na ochranu signalizácie SIP medzi UE a P-CSCF sa musí použiť ochrana integrity.

NDS

(R-CD- 16) – Ochrana integrity medzi sieťovými prvkami (napríklad medzi CSCF a medzi CSCF a HSS) sa musí spoliehať na spôsob špecifikovaný bezpečnostnou sieťovou doménou uvedenou v TS 133 210 [3].

Ut

(R-CD-17) – Medzi UE a aplikačným serverom sa musí podporovať integrita dát.

RACS

(R-CD-23) – RACS musí umožniť integritu všetkých informácií spracovaných v referenčnom bode e4.

4.4.3 Požiadavky na dôvernosť

Všeobecne

(R-CD- 18) – Dôvernosť komunikácie sa musí dosiahnuť šifrovaním. Dôvernosť uložených dát sa musí dosiahnuť šifrovaním alebo riadením prístupu.

(R-CD- 19) – Dôvernosť signalizácie a riadiacich správ sa musí zaistiť, ak si to vyžaduje aplikácia alebo prostredie, kde sú požiadavky bezpečnostnej stratégie dôverné. Mechanizmus musí umožniť výber používaného algoritmu.

Bezpečnosť prístupu

(R-CD-20) – Na signalizáciu SIP medzi UE a P-CSCF sa musí poskytovať špecifická ochrana dôvernosti IMS.

NDS

(R-CD- 21) – Ochrana dôvernosti medzi funkciami siete (napríklad medzi CSCF a medzi CSCF a HSS) sa musí spoliehať na spôsob špecifikovaný bezpečnosťou sieťovej domény uvedenej v TS 133 210 [3].

Iné špecifické požiadavky

(R-CD- 22) – Musí sa umožniť ochrana dôvernosti používateľských dát, ktoré uložil alebo spracúva poskytovateľ.

4.5 Požiadavky na súkromie

(R-P- 1) – Musí sa umožniť ochrana sieťovej topológie od ohrozenia z iných domén. Musí sa tiež umožniť bezpečnostným doménam definovanie a implementovanie ochrany pred analýzami prevádzky signalizačných a riadiacich protokolov.

(R-P- 2) – Lokalita používateľa a charakteristiky využívania sa musia chrániť pred neželaným odhalením.

(R-P- 3) – Musí sa umožniť ochrana dôvernosti identifikačných dát používateľa.

(R-P- 4) – V NGN sa musia podporovať anonymné komunikačné relácie, jednak v trvalom režime, alebo v dočasnom režime komunikácie pri volaní. V tom prípade identifikácia volajúcej strany sa nesmie prezentovať na strane volaného. Sieť, ku ktorej je volaná strana pripojená, je zodpovedná za spracovanie tejto služby.

(R-P- 5) – NGN musí podporiť špecifický prípad, ak volaná strana má nadradené právo (napríklad komunikačné relácie tiesňových volaní). Identifikácia volajúcej strany sa poskytuje k volanej strane nezávisle od toho, či je, alebo nie je táto komunikačná relácia anonymná.

(R-P- 6) – Prispôsobenie služby odmietnutie anonymnej komunikácie (ACR) musí umožniť obsluhovanému používateľovi odmietnuť prichádzajúcu komunikáciu

od používateľov alebo účastníkov, ktorí majú zamedzenú prezentáciu svojej pôvodnej identifikácie podľa prispôsobenia služby OIR.

(R-P- 7) – NGN musí pre prevádzkovateľa siete podporovať mechanizmy na garantovanie platnosti identifikácie používateľa prezentovanej v prichádzajúcom volaní k používateľovi, ak volanie je výlučne v tejto sieti prevádzkovateľa (napríklad volajúca strana a volaná strana sú účastníci jednej siete NGN).

(R-P- 8) – NGN musí poskytovať mechanizmy, ktoré umožnia prezentovať identifikáciu volajúceho v relácii, ak to volajúci nezamedzí v relácii.

(R-P- 9) – Súkromie prezentovanej informácie a potreba oprávnenia pred poskytovaním informácie o prezentácii sa musia dať konfigurovať používateľom (napríklad prítomnosť).

(R-P- 10) – Zadávateľ zobrazenia musí kontrolovať, ku komu, ako dlho a čo (celá informácia alebo jej časť) sa poskytuje z prezentovanej informácie zobrazenia, a zadávateľ sledovania musí kontrolovať, ku komu, ako dlho a čo (celá informácia alebo jej časť) sa prezentuje zo sledovanej informácie sledovateľa.

(R-P- 11) – Akékoľvek služby používajúce informáciu o prezentácii musia zaručiť súhlas s telekomunikačným tajomstvom pred uvoľnením informácie o prezentácii. Charakter služby neurčuje špecifické problémy využívania (napríklad, kde je uložený a ako je dohodnutý súhlas). Uvádza len požiadavky na administratívne riadenie súkromia.

(R-P- 12) – Musí sa pre vysielateľa správy požadovať zamedzenie jeho verejnej identifikácie pre prijímateľa.

(R-P- 13) – Používatelia môžu zrušiť prezentovanú identifikáciu, ak začínajú reláciu alebo vysielajú správu. Musí sa umožniť overovanie identifikácie a reakcia iniciovaním relácie alebo správy.

4.6 Strategické požiadavky na riadenie

(R-KM- 1) – Riadenie a distribúcia kľúča medzi SEGF musí vyhovovať bezpečnosti sieťovej domény podľa TS 133 210 [3].

(R-KM- 2) – UE a AS musia obnoviť predtým vytvorenú bezpečnú reláciu.

(R-KM- 3) – Riadiaci mechanizmus kľúča musí prechádzať cez zariadenie NAT/NATP.

4.7 Požiadavky na bezpečné riadenie

POZNÁMKA. – Požiadavky na bezpečné riadenie sa naďalej študujú.

4.8 Požiadavky na spoluprácu NAT/fireval

V tejto technickej špecifikácii sa fireval berie do úvahy vo všeobecnom zmysle. Fireval by mohol byť sieťový priechod na aplikačnej úrovni (ALG), zástupný server, filter paketov, zariadenie NAT/NATP alebo kombinácia uvedených. Funkcia bezpečnostného sieťového priechodu je jednotka na hranici bezpečnostnej domény IP a je použitá na zabezpečenie pôvodných protokolov IP na rozhraniach Za.

(R-NF- 1) – Bezpečnostné protokoly NGN musia pracovať so všeobecne používanými firevalmi a musia pracovať v prostredí s NAT/NATP.

(R-NF- 2) – Musia sa podporovať filtre paketov IP obmedzujúce/schvaľujúce prístup k špecifickým nosným tokom.

(R-NF- 3) – SEGF môže obsahovať stratégiu filtrovania a funkcie firevalu nepožadované v TS 133 210 [3].

4.9 Požiadavky na neodmietnutie

POZNÁMKA. – Požiadavky na neodmietnutie sa naďalej študujú.

4.10 Požiadavky na dostupnosť a ochranu pred DoS

(R-AD- 1) – Musí sa poskytovať mechanizmus na zníženie útokov na vyradenie služby.

(R-AD- 2) – Poskytujú sa mechanizmy riadenia prístupu na zaistenie, že len oprávnení používatelia môžu pristúpiť k službe.

(R-AD- 3) – Musí sa zamedziť votrelcom dostupnosť služieb logickými prostriedkami.

(R-AD- 4) – Musí sa poskytovať dostupnosť a presnosť lokalizačnej informácie na služby EMTEL.

(R-AD- 5) – Dostupnosť PSAP v EMTEL sa nesmie znížiť útokmi na DoS. PSAPS musí zabezpečiť opakované spojenie.

4.11 Požiadavky na zaistenie

(R-AS- 1) – NGN v TISPAN musí poskytnúť smernice na vyhodnotenie a certifikáciu zariadení a systémov NGN.

(R-AS- 2) – Následky možného chybného použitia protokolov na bezpečnosť v NGN sa musia dokumentovať cez TVRA. To umožňuje používateľom odhadnúť potrebnú bezpečnosť pred využívaním daného protokolu.

4.12 Požiadavky na stupeň zabezpečenia

Ak sa definujú alebo vyberajú šifrovacie algoritmy podľa TISPAN, musia sa dodržať smernice definované v EG 202 238 [4].

4.13 Požiadavky na zabezpečenie IPTV

4.13.1 Všeobecné požiadavky na bezpečnosť IPTV

POZNÁMKA. – Ak sa doručujú bezpečnostné informácie (napríklad licencie alebo kľúče) k účastníkom (špeciálne k veľkému počtu účastníkov), musí sa brať do úvahy ovplyvnenie výkonnosti systému.

(R-IPTV-C-1) – Služba IPTV v NGN musí sa brať do úvahy niekoľko druhov používateľov, pomenovaných skupín používateľov, jednotky pracujúce v mene používateľov a jednotky pracujúce v mene pomenovaných skupín používateľov.

(R-IPTV-C-2) – Služba IPTV v NGN musí prideliť používateľom jedinečné a nefalšovateľné používateľské identifikácie.

(R-IPTV-C-3) – Služba IPTV v NGN musí umožniť pre viacerých používateľov (rozhodne sa o počte) priradenie k jednému predplatnému.

(R-IPTV-C-4) – Služba IPTV v NGN musí jednoznačne overiť totožnosť všetkých používateľov služby IPTV pomocou jednoznačných a nefalšovateľných poverení na overovanie totožnosti na základe predplatného.

(R-IPTV-C-5) – Služba IPTV v NGN musí jednoznačne autorizovať všetkých používateľov na základe predplatného.

(R-IPTV-C-6) – Služba IPTV v NGN musí priradiť jednoznačné a nefalšovateľné identifikácie k všetkým účastníkom a pomenovaným skupinám účastníkov.

(R-IPTV-C-7) – Služba IPTV v NGN musí jednoznačne overiť totožnosť všetkých účastníkov a pomenovaných skupín účastníkov o službu IPTV pomocou jednoznačných poverení na overovanie totožnosti.

(R-IPTV-C-8) – Služba IPTV v NGN musí jednoznačne autorizovať všetkých účastníkov a pomenovaných skupín účastníkov o službu IPTV.

(R-IPTV-C-9) – Služba IPTV v NGN musí priradiť jednoznačné a nefalšovateľné identifikácie k všetkým používateľským zariadeniam.

(R-IPTV-C-10) – Služba IPTV v NGN musí jednoznačne autorizovať všetky zariadenia o službu IPTV.

(R-IPTV-C-11) – Služba IPTV v NGN musí priradiť jednoznačné a nefalšovateľné identifikácie k všetkým reláciám IPTV, ktoré kontrolujú používatelia a zariadenia.

(R-IPTV-C-12) – Služba IPTV v NGN musí priradiť jednoznačné a nefalšovateľné identifikácie k všetkým poskytovateľom služby IPTV, ktoré kontrolujú používatelia.

(R-IPTV-C-13) – Služba IPTV v NGN musí poskytnúť mechanizmus na overovanie totožnosti a autorizáciu riadiacich správ RTSP od používateľov.

(R-IPTV-C-14) – Služba IPTV v NGN musí priradiť jednoznačné a nefalšovateľné identifikácie k celému obsahu IPTV, ktorý kontrolujú používatelia.

4.13.2 Požiadavky na ochranu služby IPTV

(R-IPTV-CN-1) – Funkcie bezpečnostnej služby IPTV v NGN musia podporiť distribúciu prístupových kľúčov prichádzajúcich zo siete podľa zodpovedajúcich práv.

(R-IPTV-CN-2) – Funkcie bezpečnostnej služby IPTV v NGN musia podporiť prostriedky na ochranu kľúčov priradených k službe proti neoprávnenému prístupu a umožniť ich integritu a dôvernosť.

(R-IPTV-CN-3) – Funkcie bezpečnostnej služby IPTV v NGN musia overiť totožnosť a zaistiť integritu a dôveryhodnosť komunikácie medzi službou a používateľom.

(R-IPTV-CN-4) – Funkcie bezpečnostnej služby IPTV v NGN musia poskytnúť prostriedky na ochranu časovo obmedzených služieb (napríklad predplatené a platené programy).

4.13.3 Požiadavky na ochranu obsahu IPTV

(R-IPTV-CP-1) – Ochrana obsahu IPTV v NGN musí overiť totožnosť a autorizovať vytvorenie celého obsahu IPTV k prijímajúcim používateľom.

(R-IPTV-CP-2) – Ochrana obsahu IPTV v NGN musí overiť pôvodnosť vytvoreného celého obsahu k prijímajúcim používateľom.

(R-IPTV-CP-3) – Ochrana obsahu IPTV v NGN musí poskytovať ochranu dôvernosti obsahu medzi koncovými bodmi siete v medziach regulácie.

(R-IPTV-CP-4) – Služba IPTV v NGN musí poskytovať ochranu integrity obsahu medzi koncovými bodmi siete v relácii IPTV.

(R-IPTV-CP-5) – Služba IPTV v NGN musí kontrolovať a obmedziť obsah na základe obsahu metadát pre používateľov.

(R-IPTV-CP-6) – Služba IPTV v NGN a funkcie ochrany obsahu musia poskytovať prostriedky na obnovu súvisiacich práv alebo kľúčov vo vybratých chránených položkách obsahu.

(R-IPTV-CP-7) – Služba IPTV v NGN musí mať opatrenie na zamedzenie neautorizovaného použitia obsahu (prehliadanie, opakované prehliadanie, kopírovanie a pod.) používateľmi.

(R-IPTV-CP-8) – Služba IPTV v NGN musí mať opatrenie na zamedzenie neautorizovaného šírenia obsahu používateľmi.

(R-IPTV-CP-9) – Funkcie ochrany obsahu IPTV v NGN musia poskytnúť prostriedky na ochranu časovo obmedzeného použitia obsahu.

4.13.4 Požiadavky na bezpečnosť IPTV v prostredí IMS

POZNÁMKA. – Musí sa uvažovať s opakovaným použitím existujúcich bezpečnostných mechanizmov IMS, toľkých, koľko je nevyhnutné.

4.13.5 Požiadavky na bezpečnosť IPTV v prostredí inom, ako je IMS

(R-IPTV-NIMS-1) – Služba IPTV v NGN musí v každej relácii IPTV jednoznačne spojiť zariadenia, používateľov, pomenované skupiny používateľov, jednotky pracujúce v mene používateľov k reláciám IPTV.

(R-IPTV-NIMS-2) – Služba IPTV v NGN musí v každej kombinovanej relácii IPTV jednoznačne pripojiť zariadenia, používateľov k relácii IPTV.

(R-IPTV-NIMS-3) – Služba IPTV v NGN musí priradiť jednoznačné identifikácie k logike kritickej služby IPTV na zariadenia, ktoré kontrolujú používatelia.

(R-IPTV-NIMS-4) – Služba IPTV v NGN musí priradiť nezabudnuteľné identifikácie k logike kritickej služby IPTV na zariadenia, ktoré kontrolujú používatelia.

(R-IPTV-NIMS-5) – Služba IPTV v NGN musí overiť totožnosť a autorizovať logiku kritickej služby IPTV na zariadenia, ktoré kontrolujú používatelia.

(R-IPTV-NIMS-6) – Služba IPTV v NGN musí overiť pôvodnosť logiky kritickej služby IPTV na zariadenia, ktoré kontrolujú používatelia.

(R-IPTV-NIMS-7) – Zlepšenie DSF9: Služba IPTV v NGN musí jednoznačne overiť totožnosť všetkých účastníkov a pomenovaných skupín účastníkov, ak pristúpia k súkromným a dôverným informáciám pomocou jednoznačných poverení na overovanie totožnosti.

(R-IPTV-NIMS-8) – Zlepšenie DSF 10: Služba IPTV v NGN musí jednoznačne autorizovať všetkých účastníkov a pomenovaných skupín účastníkov, ak pristúpia k súkromným a dôverným informáciám.

(R-IPTV-NIMS-9) – Služba IPTV v NGN musí poskytovať šifrovanie medzi koncovými bodmi pri súkromných alebo dôverných informáciách na základe relácie IPTV.

4.13.6 Požiadavky na dostupnosť a ochranu pred DoS

(R-IPTV-AD-1) – Služba IPTV v NGN musí byť dostupná pre autorizovaných používateľov, účastníkov a zariadenia podľa požiadaviek služby IPTV vzhľadom na včasnosť a kvalitu.

(R-IPTV-AD-2) – Služba IPTV v NGN musí mať opatrenie na zamedzenie útokov DoS na službu IPTV aby bolo zaistené splnenie požiadaviek služby IPTV vzhľadom na včasnosť a kvalitu.

(R-IPTV-AD-3) – Služba IPTV v NGN musí mať opatrenie na detekciu a činnosť po všetkých útokoch DoS na službu IPTV (znamená to, že činnosť môže mať význam informovať, napríklad administrátora systému udalosti) na zaistenie splnenia požiadaviek služby IPTV vzhľadom na včasnosť a kvalitu.

4.14 DRM

(R-IPTV-DRM-1) – Služba IPTV v NGN musí poskytovať všeobecný rámec otvorený na integráciu riešení ochrany obsahu (DRM).

(R-IPTV-DRM-2) – Jedno alebo viac otvorených úplne štandardizovaných riešení DRM sa musí podporovať s ochranou obsahu IPTV v NGN vrátane napríklad riadenia kľúča, doručenia a šifrovania a dešifrovania činností kľúčov a obsahu a rozhraní. Všetky riešenia musia byť úplne špecifikované, pripúšťajúce veľmi dobre definované varianty v prevádzkovom správaní bez zavedenia výhradných prvkov do každej časti systému. Všetky takéto riešenia musia mať rovnakú prioritu.

(R-IPTV-DRM-3) – Úplne štandardizované riešenie DRM musí splniť požiadavky určené v článku 4.13.3 Požiadavky na ochranu obsahu IPTV.

4.15 Požiadavky na bezpečnosť média

4.15.1 Všeobecné požiadavky na bezpečnosť média

4.15.1.1 Regulačné požiadavky

(R-MS-REG-1) – NGN musí poskytovať mechanizmus na zabránenie odpočúvania prevádzky.

(R-MS-REG-2) – NGN musí poskytovať mechanizmus na zabránenie neoprávneného nahrávania a ukladania prevádzky.

(R-MS-REG-3) – NGN musí poskytovať mechanizmus na zabránenie neoprávneného zachytávania prevádzky.

(R-MS-REG-4) – Prevádzkovateľ NGN musí poskytovať mechanizmus na umožnenie zachytávania a presmerovania signalizácie špecifických používateľov NGN, ak to požaduje oprávnený úrad.

POZNÁMKA 1. – Požiadavka sa netýka len média, ale môže sa korelovať na zabezpečenie média.

(R-MS-REG-5) – Prevádzkovateľ NGN musí poskytovať mechanizmus umožňujúci zachytávanie a presmerovanie obsahu komunikácie špecifických používateľov NGN, ak to požaduje oprávnený úrad.

(R-MS-REG-6) – Prevádzkovateľ NGN musí poskytovať mechanizmus umožňujúci zachovanie a presmerovanie signalizácie špecifických používateľov NGN, ak to požaduje oprávnený úrad.

POZNÁMKA 2. – Požiadavka sa netýka len média, ale môže sa korelovať na zabezpečenie média.

4.15.1.2 Nie vysielacie mediálne trasy

(R-MS-GEN-1) – NGN musí umožniť, aby neširokopásmové mediálne trasy boli konštruované tak, že odpočúvanie sa nedá dosiahnuť bez napojenia sa do mediálnej trasy.

(R-MS-GEN-2) – NGN musí umožniť, že vysielacie mediálne trasy (napríklad rádio) musia byť chránené šifrovaním mediálneho obsahu.

(R-MS-GEN-3) – NGN musí umožniť, že kľúč použitý na šifrovanie je známy len stranám priamo zainteresovaným na prenose média vo vysielacej trase.

4.15.1.3 Požiadavky na NGN

(R-MS-1) – NGN musí zabezpečiť podporu na bezpečnosť medzi mediálnymi koncovými bodmi.

(R-MS-2) – NGN musí zabezpečiť podporu na bezpečnosť média používateľ – sieť (nasledovných bezpečnostných služieb, ako sú dôvernosť, integrita, hodnovernosť zdrojových a cieľových koncových bodov).

(R-MS-3) – NGN musí zabezpečiť podporu na bezpečný mediálny prenos (prenos v médiu) v topológiách bod-bod.

(R-MS-4) – NGN musí zabezpečiť podporu na bezpečný prenos média v topológiách bod-viacbodov.

(R-MS-5) – NGN musí zabezpečiť podporu na bezpečný prenos média vo vysielacích topológiách.

(R-MS-6) – NGN musí zabezpečiť mechanizmus na zamedzenie odpočúvania prevádzky.

(R-MS-7) – NGN musí zabezpečiť mechanizmus na zamedzenie neoprávneného zaznamenávania a ukladania prevádzky.

(R-MS-8) – NGN musí zabezpečiť mechanizmus na zamedzenie neoprávneného zachytávania prevádzky.

(R-MS-9) – NGN musí umožniť, aby neširokopásmové mediálne trasy boli konštruované tak, že odpočúvanie sa nedá dosiahnuť bez napojenia na mediálnu trasu.

(R-MS-10) – NGN musí umožniť, že vysielacie mediálne trasy (napríklad rádio) musia byť chránené šifrovaním mediálneho obsahu.

(R-MS-11) – NGN musí umožniť, že kľúč použitý na kryptovanie je známy len stranám priamo zainteresovaným na prenose média vo vysielacej trase.

4.15.1.4 Požiadavky na NGCN

(R-NGCN-1) – NGN musí poskytovať podporu na zabezpečený prenos média medzi NGCN a NGN.

(R-NGCN-2) – NGCN musí umožniť, aby médiá boli bezpečné (šifrované, dôveryhodné a s chránenou integritou) transparentne medzi koncovými bodmi alebo koncovým bodom k sieťovému priechodu PSTN/ISDN s výnimkou, ak vznikne požadovaný alebo oprávnený zásah v médiách.

(R-NGCN-3) – NGCN musí byť transparentná k riadeniu kľúča na zabezpečenie média umiestneného medzi koncovými zariadeniami (alebo koncovým zariadením k sieťovému priechodu PSTN/ISDN), s evidenciou šifrovania, že partner príslušný na spracovanie kľúča alebo na dohodu o kľúči je predpokladaný komunikačný partner.

(R-NGCN-4) – NGCN musí byť transparentná pri šifrovaní medzi koncovými bodmi akejkoľvek výmeny kľúča požadovanej na zabezpečenie média.

4.15.2 Požiadavky na bezpečnosť média v prostredí IMS

Nedefinované.

POZNÁMKA. – Tento článok môže byť spracovaný na účely verzie 2.

4.15.3 Požiadavky na bezpečnosť média v inom prostredí, ako je IMS

Nedefinované.

POZNÁMKA. – Tento článok môže byť spracovaný na účely verzie 2.

4.16 Požiadavky na zabezpečenie registrácie nežiadanej komunikácie

(R-UC-1) – NGN musí poskytovať prostriedky pre používateľov NGN na hlásenie volaní ako UC.

(R-UC-2) – Hlásenia UC vytvorené používateľmi UC musí kontrolovať NGN.

(R-UC-3) – NGN musí poskytovať schopnosť pre napadnutého používateľa požadovať klasifikovanie volania UC.

(R-UC-4) – NGN musí poskytovať schopnosť pre napadnutého používateľa odmietnuť klasifikovanie vytvorené detekčným systémom UC.

R-UC-5 – NGN musí poskytovať schopnosť napadnutému CSP vybrať zo signalizácie volania dostatočnú informáciu na poskytovanie klasifikácie UC volania.

R-UC-6 – NGN musí poskytovať mechanizmus na prenos klasifikácie UC v signalizácii volania.

R-UC-7 – NGN musí poskytovať mechanizmus na umožnenie zmien v spracovaní volania s osobitnou klasifikáciou UC.

4.17 Požiadavky na zabezpečenie podnikovej komunikácie

Nedefinované.

POZNÁMKA. – Tento článok môže byť spracovaný na účely verzie 2.

4.17.1 Všeobecné požiadavky na bezpečnosť

Nedefinované.

4.17.2 Špecifické požiadavky na bezpečnosť prepojenia NGN/NGCN

Nedefinované.

4.17.3 Špecifické požiadavky na bezpečnosť v hostiteľských podnikových službách

Nedefinované.

4.17.4 Špecifické požiadavky na bezpečnosť v podnikových okruhových aplikáciách

Nedefinované.

4.17.4.1 Požiadavky na bezpečnosť (predplatené) v podnikových okruhových aplikáciách

Nedefinované.

4.17.4.2 Požiadavky na bezpečnosť v podnikových okruhových aplikáciách (medzi partnermi)

Nedefinované.

4.17.5 Špecifické požiadavky na bezpečnosť vo virtuálnych prenajatých okruhoch

Nedefinované.

4.18 Požiadavky na bezpečnosť NAT Traversal

(R-NAT TRAV-1) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať priečku ďalej uvedeného typu správania NAT medzi UE a chrbticovou sieťou IMS:

- mapovanie nezávislé od koncového bodu,
- mapovanie podľa adresy,
- mapovanie podľa adresy a portu.

(R-NAT TRAV-2) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať tieto druhy filtrovania medzi UE a chrbticovou sieťou IMS:

- filtrovanie nezávislé od koncového bodu,
- filtrovanie nezávislé od adresy,
- filtrovanie podľa adresy a portu.

(R-NAT TRAV-3) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať pásmové a mimopásmové požiadavky k UE cez jedno alebo viac zariadení NAT.

(R-NAT TRAV-4) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať jednosmernú a obojsmernú prevádzku RTP.

(R-NAT TRAV-5) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať spojenie TCP inicializované externe a interne.

(R-NAT TRAV-6) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať miestne siete.

(R-NAT TRAV-7) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať IPv4.

(R-NAT TRAV-8) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať IPv6.

(R-NAT TRAV-9) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať individuálnu prevádzku.

(R-NAT TRAV-10) – Priečka NAT podľa NGN R2 v TISPAN musí minimalizovať počet správ, ktoré sa prenášajú záväzne cez priečku NAT.

(R-NAT TRAV-11) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať viac UE (jedno alebo viac zariadení) za jedným NAT.

(R-NAT TRAV-12) – Priečka NAT podľa NGN R2 v TISPAN musí minimalizovať dodatočné oneskorenie vytvorenej relácie.

(R-NAT TRAV-13) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať priečku IMS.

(R-NAT TRAV-14) – Priečka NAT podľa NGN R2 v TISPAN musí podporovať signalizáciu SIP šifrovanú v IPsec.

(R-NAT TRAV-15) – Priečka NAT podľa NGN R2 v TISPAN musí brať do úvahy modulárnosť, komplexnosť a kompatibilitu s inými dôležitými požiadavkami NGN.

(R-NAT TRAV-16) – Akékoľvek riešenie odporúčané pri priečke NAT nesmie ovplyvniť základnú schopnosť TLS pracovať cez NAT.

4.19 Požiadavky na bezpečnosť siete v domácnosti

Nedefinované.

POZNÁMKA. – Tento článok môže byť spracovaný na účely verzie 2.

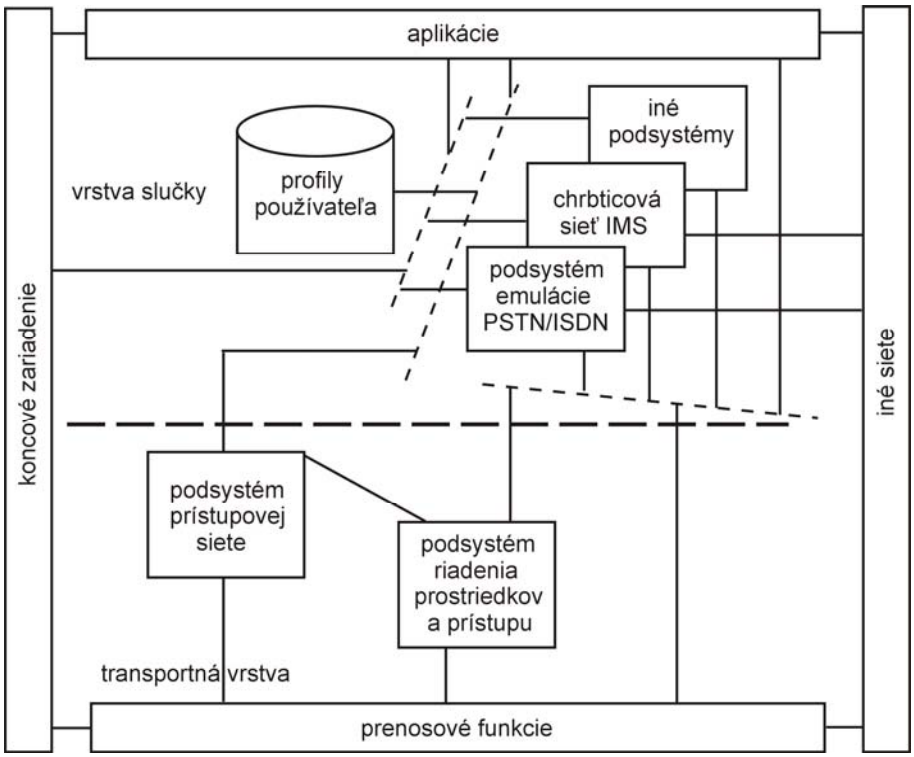
4.20 Požiadavky na bezpečnosť H.248

Nedefinované.

POZNÁMKA. – Tento článok môže byť spracovaný na účely verzie 2.

5 Mapovanie požiadaviek na bezpečnosť – verzia 2

Kapitola 5 mapuje bezpečnostné požiadavky určené v kapitole 4 na aplikáciu podsystémov NASS, RACS, IMS a PES, ako aj aplikačného servera a rozhraní. Kapitola 5 sa považuje za informatívnu kapitolu na uľahčenie zaznamenávania požiadaviek podľa rozhrania a podsystému.



Obrázok 1 – Celková architektúra TISPAN NGN

5.1 Podsystém prístupovej siete (NASS)

Požiadavky súvisiace s požiadavkami bezpečnosti NASS

Požiadavky na bezpečnosť
(R-AA- 24) – NASS musí podporovať použitie explicitného (napríklad PPP alebo IEEE 802.1X) alebo implicitného overenia spoja (napríklad overovanie totožnosti adresy MAC alebo overovanie totožnosti spojenia) používateľmi/účastníkmi. V prípade implicitného overenia totožnosti sa musí spoliehať na implicitné overovanie totožnosti fyzickou alebo logickou identifikáciou na transportnej vrstve 2 (L2).
(R-AA- 25) – V prípade, ak je CNG smerovací modem a sieť na strane účastníka (CPN) je privátna oblasť IP, overovanie totožnosti sa musí iniciovať z CNG.
(R-AA- 26) – V prípade, ak je CNG mostík, každé UE musí overiť totožnosť s NASS, ak oblasť IP v CPN rozpozná prístupná sieť.
(R-AA- 3) – V nie starších rozvojových variantoch overovanie totožnosti IMS musí byť nezávislé od overenia totožnosti na prístupe.
(R-AA- 7) – Musí sa umožniť zamedzenie použitia osobitnej ISIM na prístup k sieťam a službám NGN a musí sa umožniť zrušenie špecifického ISIM.

(R-AA-11) – Ak prevádzkovateľ IMS v NGN využíva riešenia Digest a ISIM, potom prevádzkovateľ musí určiť mechanizmus overenia totožnosti (SIP Digest alebo ISIM) pre každého používateľa. Mechanizmus overenia totožnosti sa musí využívať podľa informácie o predplatnom v profile služby používateľa a špecifickej stratégie prevádzkovateľa IMS v NGN. Ak koncové zariadenie podporuje riešenie ISIM a prevádzkovateľ siete podporuje riešenia ISIM a staršie riešenia, musí sa použiť riešenie ISIM.
(R-AA- 12) – Prenášané heslá sa musia vhodne chrániť, napríklad šifrovaním alebo inými spôsobmi.
(R-AA- 13) – V špeciálnych starších rozvojových variantoch (pozri poznámku 1), kde overovanie totožnosti IMS je spojené s overením totožnosti na prístupe, musí sa umožniť získanie prístupu k službám IMS po procedúre overenia totožnosti. Overovanie totožnosti poskytuje súbežný prístup k prístupovej sieti a službám IMS. POZNÁMKA 1. – Existujú dva špeciálne varianty staršieho rozvoja (takisto súvisiace s overením totožnosti NASS Bundled): (A) – Overovanie totožnosti je spojené s overením totožnosti prístupového spoja (bez putovania). (B) – Overovanie totožnosti je spojené s overením totožnosti prístupu na spojenie IP (môže sa poskytovať obmedzené putovanie). POZNÁMKA 2. – Overovanie totožnosti na prístupe môže spôsobiť v službách IMS pripojenie k prístupovému bodu (spoju) alebo k poslednému spojeniu IP (zariadeniu). V druhom prípade môže byť dostupné obmedzenie putovania. Na získanie prístupu k službám IMS sa nepožaduje špecifické overovanie totožnosti IMS od CPE/koncového zariadenia.
(R-AA- 14) – Podsystémy NGN musia definovať a vykonávať stratégiu vzhľadom na právoplatnosť overenia totožnosti používateľa.
(R-AA- 20) – Medzi CPE a NASS sa musí podporovať vzájomné overovanie totožnosti počas úrovne registrácie.
(R-AA- 21) – Prístupová sieť musí overiť totožnosť a oprávnenie účastníka na prístup.
(R-AA- 22) – Overovanie totožnosti a autorizáciu k prístupovej sieti kontroluje prevádzkovateľ prístupovej siete.
(R-AA- 23) – Atribúty požadované na overovanie totožnosti používateľa prístupovou sieťou môže poskytovať prevádzkovateľ siete, u ktorého má predplatné používateľ IMS v NGN.
(R-AA- 29 – Identifikácia volajúceho a informácia o lokalite sa musia uložiť podľa všeobecného európskeho regulačného rámca poskytovateľom služby EMTEL. Identifikáciu volajúceho a informáciu o lokalite musí potvrdiť poskytovateľ služby EMTEL.
(R-SP- 1) – Sieť NGN podľa TISPAN sa musí logicky a fyzicky rozdeliť do bezpečnostných domén umožňujúcich oddelenie aplikácie (napríklad IMS) a prenosu (napríklad ADSL alebo UMTS). Aj rozličníprevádzkovatelia podobných sietí (napríklad IMS) musia vykonávať svoju vlastnú bezpečnostnú stratégiu.
(R-SP- 3) – Bezpečnostný mechanizmus musí byť rozdelený tak, aby funkcie overenia totožnosti, dátovej integrity, opakovania detekcie a dôvernosti mohli sa implementovať a vybrať navzájom nezávisle podľa významu.
(R-IR- 2) – Na overovanie totožnosti prístupu sa musí použiť identifikácia prístupu. Táto identifikácia sa môže alebo nemusí použiť na iné účely.
(R-IR- 3) – Identifikácia spoja sa musí použiť na overovanie totožnosti spoja.
(R-CD- 2) – Bezpečnosť sieťovej domény (NDS) sa musí poskytovať na sieťovej vrstve a vyhovovať TS 133 210.
(R-CD- 3) – Celá prevádzka NDS/IP musí prejsť cez funkciu bezpečnostného sieťového priechodu SEGF pred vstupom do bezpečnostnej domény alebo pred jej opustením. Prevádzkovatelia IMS musia

prevádzkovať rozhranie Za v NDS/IP medzi SEGF podľa TS 133 210.
(R-CD- 7) – V tomto prípade overovanie totožnosti prístupu je nezávislé od overenia totožnosti IMS.
(R-CD- 8) – V prípade, kde overovanie totožnosti je spojené s overením totožnosti prístupového spoja, základná prístupová technológia musí poskytovať ochranu signalizácie a používateľských dát NGN.
(R-CD- 12) – Všetky dáta súvisiace s konfiguráciou UE v referenčnom bode e3 sa musia chrániť pred stratou dôveryhodnosti a stratou integrity.
(R-CD- 13) – Musí sa poskytovať ochrana integrity signalizácie, kontrola komunikácie a uložených dát.
(R-CD- 18) – Dôvernosť komunikácie sa musí dosiahnuť šifrovaním. Dôvernosť uložených dát sa musí dosiahnuť šifrovaním alebo kontrolou prístupu.
(R-CD- 19) – Dôvernosť signalizácie a riadiacich správ sa musí zaistiť, ak to požaduje aplikácia alebo prostredie, kde bezpečnostná stratégia požaduje dôvernosť. Mechanizmus musí umožniť výber použitého algoritmu.
(R-CD- 22) – Musí sa umožniť ochrana dôvernosti používateľských dát, ktoré uložil alebo spracúva prevádzkovateľ.
(R-P- 1) – Musí sa umožniť ochrana sieťovej topológie od ohrozenia z iných domén. Musí sa takisto pri bezpečnostných doménach definovať a implementovať ochrana pred analýzami prevádzky signalizačných a riadiacich protokolov.
(R-P- 2) – Lokalita používateľa a charakteristiky využívania sa musia chrániť pred neželaným odhalením.
(R-P- 3) – Musí sa umožniť ochrana dôvernosti identifikačných údajov používateľa.
(R-P- 5) – NGN musí podporiť špecifický prípad, ak volaná strana má právo zamedzenia (napríklad komunikačné relácie tiesňových volaní), identifikácia volajúcej strany sa poskytuje k volanej strane nezávisle od toho či je, alebo nie je táto komunikačná relácia anonymná.
(R-P- 7) – NGN musí pre prevádzkovateľa siete podporovať mechanizmy na garantovanie platnosti identifikácie používateľa prezentovanej v prichádzajúcom volaní k používateľovi, ak volanie je výlučne v tejto sieti prevádzkovateľa (napríklad volajúca strana a volaná strana sú účastníci jednej siete NGN).
(R-P- 8) – NGN musí poskytovať mechanizmy, ktoré umožnia prezentovať identifikáciu volajúceho v relácii, ak to nie je volajúcim zamedzené v relácii.
(R-KM- 3) – Mechanizmus riadenia kľúča musí prejsť zariadenie NAT/NATP.
(R-NF- 1) – Bezpečnostné protokoly NGN musia pracovať so všeobecne používanými firevalmi a musia pracovať v prostredí s NAT/NATP.
(R-NF- 2) – Musia sa podporovať filtre paketov IP na zamedzenie/schválenie prístupu k špecifickým nosným tokom.
(R-AD- 1) – Musí sa poskytovať mechanizmus na zníženie útokov na vyradenie služby.
(R-AD- 2) – Poskytujú sa mechanizmy riadenia prístupu na zaistenie, že len oprávnení používatelia môžu pristúpiť k službe.
(R-AD- 3) – Musí sa zamedziť narušiteľom zamedzenie dostupnosti k službám logickými prostriedkami.
(R-AD- 4) – V službách EMTEL sa musí poskytovať dostupnosť a presnosť informácie o lokalite.
(R-AD- 5) – Dostupnosť PSAP EMTEL sa nesmie znížiť útokmi DoS. PSAP EMTEL musia mať schopnosť opakovania spojenia.
(R-AS- 1) – NGN v TISPAN musí poskytnúť smernice na vyhodnotenie a certifikáciu zariadení a systémov NGN.

(R-AS- 2) – Následky možného chybného použitia protokolov na bezpečnosť v NGN sa musia dokumentovať cez TVRA. To umožňuje používateľom odhadnúť potrebnú bezpečnosť, pred využívaním daného protokolu.

5.2 Podsystém riadenia prostriedkov a prístupu (RACS)

Požiadavky súvisiace s požiadavkami na bezpečnosť RACS

Požiadavky na bezpečnosť
(R-AA- 27) – RACS a AF si musia vzájomne overiť totožnosť pred autorizáciou prostriedkov.
(R-AA- 27A) – AF a SDF v RACS musia mať schopnosť vzájomnej identifikácie, ak sa vykonáva overovanie totožnosti.
(R-CD- 17) – RACS musí zaistiť integritu celej stratégie vzhľadom na informáciu o prostriedkoch vymieňanú medzi NASS a RACS. POZNÁMKA 1. – Požaduje sa, že RACS je overovateľ integrity vymieňaných dát a NASS je generátor kontroly integrity dát.
(R-CD- 18) – Platnosť integrity dát v RACS sa musí vykonávať pomocou Message Digest (MD) alebo šifrovaním správy na overovanie totožnosti (MAC) s kľúčmi odvodenými podľa osobitných jednoznačných identifikátorov v aplikačnej vrstve AF a SPDF (ako sa definuje v R-AA-28). POZNÁMKA 2. – Osobitné jednoznačné identifikátory v aplikačnej vrstve sa špecifikujú v požiadavke R-AA-28 a sú podmienkou v R-CD-17 a R-CD-18.

5.3 Chrbtica multimediálneho podsystému IP (IMS)

Požiadavky súvisiace s požiadavkami na bezpečnosť chrbticovej siete IMS

Požiadavky na bezpečnosť
(R-AA- 1) – Prístup k sieťam, službám a aplikáciám NGN sa musí umožniť len oprávneným používateľom.
(R-AA- 3) – V nie starších rozvojových variantoch, overovanie totožnosti musí byť nezávislé od overenia totožnosti na prístupe.
(R-AA- 4) – ISIM sa musí použiť na prístup k akejkoľvek službe, ale výnimky sa môžu povoliť na tiesňové volania a staršie rozvojové varianty.
(R-AA- 5) – Overovanie totožnosti založené na ISIM medzi účastníkom IMS a sieťou musí vyhovieť časti overenia totožnosti bezpečnosti na prístupe k službám IP podľa TS 133 203.
(R-AA- 6) – Opakované overovanie totožnosti účastníka IMS musí vyhovieť časti overenia totožnosti bezpečnosti na prístupe k službám IP podľa TS 133 203.
(R-AA- 7) – Musí sa zabrániť použitiu osobitnej ISIM k prístupu sietí a služieb NGN a musí sa umožniť zrušenie špecifickej ISIM.
(R-AA- 8) – Špecifická informácia ISIM dôležitá na NGN sa musí chrániť pred neoprávneným prístupom alebo zmenou.
(R-AA- 9) – Overovanie totožnosti môže byť hardvérové (3GPP UE: ISIM; napríklad skúška pomocou fyzického znamienka) alebo softvérové (skúška poznaním určitej utajenej informácie).
(R-AA- 10) – Overovanie totožnosti k IMS v NGN pomocou mechanizmu SIP Digest sa musí podporovať ako variant staršieho rozvoja.

(R-AA-11) – Ak prevádzkovatelia IMS v NGN využívajú riešenia Digest a ISIM, potom prevádzkovateľ musí určiť mechanizmus overenia totožnosti (SIP Digest alebo ISIM) pre každého konkrétneho používateľa. Mechanizmus overenia totožnosti sa musí využívať podľa informácie o predplatnom v profile používateľskej služby a špecifickej stratégie prevádzkovateľa IMS v NGN. Ak koncové zariadenie podporuje riešenie ISIM a prevádzkovateľ siete podporuje aj ISIM, aj staršie rozvojové riešenie, musí sa použiť riešenie ISIM.
(R-AA- 12) – Prenášané heslá sa musia dostatočne chrániť, napríklad šifrovaním alebo inými spôsobmi.
(R-AA- 13) – V špeciálnych starších rozvojových variantoch (pozri poznámku 1), kde overovanie totožnosti IMS je spojené s overením totožnosti na prístupe, musí sa umožniť získanie prístupu k službám IMS po procedúre overenia totožnosti. Overovanie totožnosti poskytuje súčasný prístup k prístupovej sieti a k službám IMS. POZNÁMKA 1. – Existujú dva špeciálne staršie rozvojové varianty (takisto súvisiace s overením totožnosti NASS Bundled): (A) – Overovanie totožnosti je spojené s overením totožnosti k prístupovému spoju (bez putovania) (B) – Overovanie totožnosti IMS je spojené s overením totožnosti prístupu na spojenie IP (môže sa umožniť obmedzene putovanie). POZNÁMKA 2. – Overovanie totožnosti na prístupe môže spôsobiť v službách IMS pripojenie k prístupovému bodu (spoju) alebo k poslednému spojeniu IP (zariadeniu). V druhom prípade obmedzené putovanie môže byť dostupné. Nepožaduje sa špecifické overovanie totožnosti IMS od CPE/koncového zariadenia na získanie prístupu k službám IMS.
(R-AA- 14) – Podsystémy NGN musia mať schopnosť definovať a vykonávať stratégiu vzhľadom na platnosť overenia totožnosti používateľa.
(R-AA- 23) – Atribúty požadované na overovanie totožnosti používateľa prístupovou sieťou môže poskytnúť prevádzkovateľ siete, u ktorého má používateľ predplatné IMS v NGN.
(R-AA- 25) – V prípade, kde CNG je smerovací modem a sieť na strane účastníka (CPN) je privátna oblasť IP, overovanie totožnosti sa musí inicializovať z CNG.
(R-AA- 28) – Overovanie totožnosti používateľov NGN a overovanie totožnosti koncových zariadení musí byť samostatné.
(R-AA- 29) – Identifikácia volajúceho a informácia o lokalite sa musia uložiť podľa všeobecného európskeho regulačného rámca poskytovateľom služby EMTEL. Identifikáciu volajúceho a informáciu o lokalite musí potvrdiť poskytovateľ služby EMTEL.
(R-SP- 1) – Sieť NGN podľa TISPAN musí byť logicky a fyzicky rozdelená na bezpečnostné domény umožňujúce oddelenie aplikácie (napríklad IMS) a prenosu (napríklad, ADSL alebo UMTS). Aj rozličnί prevádzkovatelia podobných sietí (napríklad IMS) musia byť schopní prevádzkovať svoju vlastnú bezpečnostnú stratégiu.
(R-SP- 2) – Bezpečnostné mechanizmy a iné parametre prednastavené mechanizmami bezpečnosti sa musia konfigurovať. To musí byť nemenné v rozhraní NNI a môže sa dohodnúť v rozhraniach UNI. Dohodnutie bezpečnostného mechanizmu musí mať určitú minimálnu úroveň definovanú bezpečnostnou doménou; napríklad zamedzenie útokov na vyradenie ponuky. Používatelia musia byť schopní zrušiť komunikáciu, ktorá nespĺňa ich minimálnu stratégiu bezpečnosti.
(R-SP- 3) – Bezpečnostný mechanizmus sa musí rozdeliť tak, aby funkcie overenia totožnosti, dátovej integrity, opakovania detekcie a dôvernosti sa mohli implementovať a vybrať navzájom nezávisle podľa významu.
(R-SP- 4) – UE musí vždy ponúkať šifrovací algoritmus na P-CSCF. Aby sa použil v reláciách a stratégii P-CSCF, musí sa definovať, či použiť šifrovanie, alebo nie.
(R-SP- 5) – UE a P-CSCF si musia dohodnúť algoritmus integrity, ktorý sa musí použiť v relácii.
(R-SP- 6) – Stratégia HN sa musí použiť na rozhodnutie, či overovanie totožnosti sa vykoná na registráciu rozličných IMPU, napríklad patriacich do rovnakých alebo odlišných profilov služby.

(R-SP- 7) – Funkcie bezpečnostného sieťového priechodu (SEGF) musia vykonávať bezpečnostnú stratégiu pri spolupráci medzi sieťami.
(R-SP- 8) – SEGF sú zodpovedné za bezpečnosť citlivých činností a z dlhodobého hľadiska musia ponúkať možnosti bezpečného uloženia kľúčov použitých na overovanie totožnosti IKE.
(R-IR- 1) – Musí sa umožniť implicitná registrácia IMPU. Všetky implicitne registrované IMPU patria do rovnakého profilu služby. Všetky implicitne registrované IMPU sa musia doručiť HSS k S-CSCF a následne k P-CSCF. S-CSCF musia považovať všetky implicitne registrované IMPU za registrované IMPU.
(R-IR- 2) – Na overovanie totožnosti na prístupe sa musí použiť identifikácia prístupu. Táto identifikácia sa môže, ale nemusí použiť na iné účely.
(R-CD- 1) – Dôvernosť a integrita signalizácie IMS sa musia aplikovať v režime od uzla k uzlu (UE k P-CSCF a medzi inými NE).
(R-CD- 2) – Bezpečnostná sieťová doména (NDS) sa musí poskytovať na sieťovej vrstve a vyhovieť TS 133 210 [3].
(R-CD- 3) – Celá prevádzka NDS/IP musí prechádzať cez SEGF (funkcia bezpečnostného sieťového priechodu) pred vstúpením do bezpečnostnej domény alebo pred jej opustením. Prevádzkovateľ IMS musí prevádzkovať rozhranie Za v NDS/IP medzi SEGF podľa TS 133 210 [3].
(R-CD- 4) – Bezpečnosť sa musí podporovať v sieťovej doméne na rozhraní Cx.
(R-CD- 5) – Bezpečný prístup IMS musí podporovať riešenie založené na ISIM (overovanie totožnosti, dôvernosť a ochrana integrity) na signalizáciu k používateľovi a od používateľa.
(R-CD- 6) – Medzi UE a P-CSCF sa musí poskytovať bezpečný spoj na ochranu v referenčnom bode Gm.
(R-CD- 7) – Overovanie totožnosti na prístupe je nezávislé od overenia totožnosti IMS.
(R-CD- 8) – V prípade, ak overovanie totožnosti IMS je spojené s overením totožnosti prístupového spoja, základná prístupová technológia musí poskytovať ochranu signalizácie a používateľských dát NGN.
(R-CD- 9) – Bezpečným spôsobom sa musí aktualizovať špecifická informácia ISIM.
(R-CD- 13) – Musí sa poskytovať integrita ochrany signalizácie, kontrola komunikácie a uložených dát.
(R-CD- 14) – Musí sa zaistiť pôvod, integrita a obnova dát overenia totožnosti, osobitne šifrovacieho kľúča.
(R-CD- 15) – Na ochranu signalizácie SIP medzi UE a P-CSCF sa musí použiť ochrana integrity.
(R-CD- 16) – Ochrana integrity medzi sieťovými prvkami (napríklad medzi CSCF a medzi CSCF a HSS) musí pracovať s mechanizmom špecifikovaným bezpečnostnou sieťovou doménou v TS 133 210 [3].
(R-CD- 18) – Dôvernosť komunikácie sa musí dosiahnuť šifrovaním. Dôvernosť uložených dát sa musí dosiahnuť šifrovaním alebo kontrolou prístupu.
(R-CD- 19) – Dôvernosť signalizačných a riadiacich správ sa musí zaistiť, ak to požaduje aplikácia alebo prostredie, kde bezpečnostná stratégia požaduje dôvernosť. Mechanizmus musí umožniť výber použitého algoritmu.
(R-CD- 20) – Na signalizáciu SIP medzi UE a P-CSCF sa musí poskytovať špecifická dôverná ochrana IMS.
(R-CD- 21) – Ochrana dôvernosti medzi sieťovými prvkami (napríklad medzi CSCF a medzi CSCF a HSS) musí pracovať s mechanizmom špecifikovaným bezpečnostnou sieťovou doménou uvedenou v TS 133 210 [3].
(R-CD- 22) – Musí sa umožniť ochrana dôvernosti používateľských dát, ktoré uložil alebo spravuje poskytovateľ.
(R-P- 1) – Musí sa umožniť ochrána sieťovej topológie od ohrozenia z iných domén. Musí sa takisto umožniť na

bezpečnostné domény definovanie a implementovanie ochrany pred analýzami prevádzky signalizačných a riadiacich protokolov.
(R-P- 2) – Lokalita používateľa a charakteristiky využívania sa musia chrániť pred nežiadúcim odhalením.
(R-P- 3) – Musí sa umožniť ochrana dôvernosti identifikačných údajov používateľa.
(R-P- 4) – V NGN sa musia podporovať anonymné komunikačné relácie, jednak v trvalom režime alebo v dočasnom režime komunikácie pri volaní. V tom prípade identifikácia volajúcej strany sa nesmie prezentovať na strane volaného. Sieť, ku ktorej je volaná strana pripojená, je zodpovedná za spracovanie tejto služby.
(R-P- 5) – NGN musí podporiť špecifický prípad, ak volaná strana má právo zamedzenia (napríklad komunikačné relácie tiesňových volaní). Identifikácia volajúcej strany sa poskytuje k volanej strane nezávisle od toho, či je, alebo nie je táto komunikačná relácia anonymná.
(R-P- 6) – Prispôsobenie služby (ACR) odmietnutie anonymnej komunikácie musí umožniť obsluhovanému používateľovi odmietnuť prichádzajúcu komunikáciu od používateľov alebo účastníkov, ktorí majú zamedzenú prezentáciu svojej pôvodnej identifikácie podľa prispôsobenia služby OIR.
(R-P- 7) – NGN musí podporovať pre prevádzkovateľa siete mechanizmy na garantovanie platnosti identifikácie používateľa prezentovanej v prichádzajúcom volaní k používateľovi, ak volanie je výlučne v tejto sieti prevádzkovateľa (napríklad volajúca strana a volaná strana sú účastníci jednej siete NGN).
(R-P- 8) – NGN musí poskytovať mechanizmy, ktoré umožnia prezentovať identifikáciu volajúceho v relácii, ak to nie je volajúcim zamedzené v relácii.
(R-P- 9) – Súkromie prezentovanej informácie a potreba oprávnenia pred poskytovaním informácie o prezentácii sa musia dať konfigurovať používateľom (napríklad prítomnosť).
(R-P- 10) – Príkazca prezentácie musí byť vždy schopný kontrolovať, komu, ako dlho a čo (celá informácia alebo jej časť) sa poskytuje z prezentovanej informácie prezentácie, a príkazca dohľadu musí byť vždy schopný kontrolovať, komu, ako dlho a čo (celá informácia alebo jej časť) sa poskytuje z dohľadovej informácie dohľadu.
(R-P- 11) – Akékoľvek služby používajúce informáciu o prezentácii musia zaručiť súhlas s telekomunikačným tajomstvom pred uvoľnením informácie o prezentácii. Charakter služby neurčuje špecifické problémy využívania (napríklad, kde je uložený a ako je dohodnutý súhlas). Uvádza len požiadavky na administratívne riadenie súkromia.
(R-P- 12) – Pre odosielateľa správy sa musí umožniť zamedzenie svojej verejnej identifikácie pre príjemcu.
(R-P- 13) – Používatelia môžu zrušiť prezentovanú identifikáciu, ak začínajú reláciu alebo vysielajú správu. Musí sa umožniť overovanie tejto identifikácie a reagovanie iniciovaním relácie alebo správy.
(R-KM- 1) – Riadenie kľúča a distribúcia kľúča medzi SEGF musí vyhovovať bezpečnostnej sieťovej doméne podľa TS 133 210 [3].
(R-KM- 2) – UE a AS musia obnoviť vopred zriadené bezpečné relácie.
(R-KM- 3) – Mechanizmus riadenia kľúča musí prekonať zariadenie NAT/NATP.
(R-NF- 1) – Bezpečnostné protokoly NGN musia pracovať so spoločne využívanými firevalmi a musia pracovať v prostredí NAT/NATP.
(R-NF- 2) – Musia sa podporovať filtre paketov IP na zamedzenie/schválenie prístupu k špecifickým nosným tokom.
(R-NF- 3) – SEGF môžu zahŕňať stratégiu filtrovania a funkcie firevalu nepožadované v TS 133 210 [3].
(R-AD- 1) – Musí sa poskytovať mechanizmus na zníženie útokov na vyradenie služby.
(R-AD- 2) – Poskytujú sa mechanizmy riadenia prístupu na zaistenie, že len oprávnení používatelia môžu

pristúpiť k službe.
(R-AD- 3) – Musí sa zamedziť narušiteľom zamedzenie dostupnosti služieb logickými prostriedkami.
(R-AD- 4) – Na služby EMTEL sa musí poskytovať dostupnosť a presná informácia o lokalite.
(R-AD- 5) – Dostupnosť PSAP v EMTEL sa nesmie znížiť útokmi DoS. PSAP EMTEL musí mať schopnosť opakovať spojenie.
(R-AS- 1) – NGN podľa TISPAN musí poskytnúť smernice na vyhodnotenie a certifikáciu zariadenia a systémov NGN.
(R-AS- 2) – Následky možného chybného použitia protokolov na bezpečnosť v NGN sa musia dokumentovať cez TVRA. To umožňuje používateľom odhadnúť potrebnú bezpečnosť, pred využívaním daného protokolu.

5.4 Podsystém emulácie PSTN/ISDN (PES)

Požiadavky súvisiace s požiadavkami na bezpečnosť PES

Požiadavky na bezpečnosť
(R-AA- 27) – Kontrolér mediálneho sieťového priechodu musí spracovať overovanie totožnosti z viacerých mediálnych sieťových priechodov, napríklad udržať viac bezpečnostných spojení s rozličnými mediálnymi sieťovými priechodmi.
(R-SP- 1) – Sieť NGN podľa TISPAN musí byť logicky a fyzicky rozdelená do bezpečnostných domén umožňujúcich oddelenie aplikácie (napríklad IMS) a prenosu (napríklad, ADSL alebo UMTS). Aj rozličnί prevádzkovatelia podobných sietí (napríklad, IMS) musia byť schopní prevádzkovať svoju vlastnú bezpečnostnú stratégiu.
(R-CD- 2) – Bezpečnostná sieťová doména (NDS) sa musí poskytovať sieťovou vrstvou a spĺňať požiadavky uvedené TS 133 210.
(R-CD- 3) – Celá prevádzka NDS/IP musí prejsť cez SEGF (funkcie bezpečnostného sieťového priechodu) pred vstupom do bezpečnostnej domény alebo pred odchodom z nej. Prevádzkovatelia IMS musia prevádzkovať rozhranie Za v NDS/IP medzi SEGF podľa TS 133 210.
(R-CD- 8) – V prípade, kde overovanie totožnosti je spojené s overením totožnosti prístupového spoja, základná prístupová technológia musí poskytovať ochranu signalizácie a používateľských dát NGN.
(R-CD- 13) – Musí sa poskytovať integrita ochrany signalizácie, kontroly komunikácie a uložených dát.
(R-CD- 16) – Integrita ochrany medzi sieťovými prvkami (napríklad medzi CSCF a medzi CSCF a HSS) musí využívať mechanizmus špecifikovaný bezpečnostnou sieťovou doménou podľa TS 133 210 [3].
(R-CD- 18) – Dôvernosť komunikácie sa musí dosiahnuť šifrovaním. Dôvernosť uložených dát sa musí dosiahnuť šifrovaním alebo kontrolou prístupu.
(R-CD- 19) – Dôvernosť signalizačných a riadiacich správ sa musí zaistiť, ak to požaduje aplikácia alebo prostredie, kde bezpečnostná stratégia požaduje dôvernosť. Mechanizmus musí umožniť výber použitého algoritmu.
(R-CD- 21) – Ochrana dôvernosti medzi sieťovými funkciami (napríklad medzi CSCF alebo medzi CSCF a HSS) musí využívať mechanizmus špecifikovaný bezpečnostnou sieťovou doménou uvedenou v TS 133 210 [3].
(R-CD- 22) – Musí sa umožniť ochrana dôvernosti používateľských dát, ktoré uložil alebo spracúva prevádzkovateľ.
(R-P- 1) – Musí sa umožniť ochrána sieťovej topológie od ohrozenia z iných domén. Musí sa tiež umožniť pri bezpečnostnej doméne definovať a implementovať ochranu proti analýzam prevádzky v

signalizačných a riadiacich protokoloch.
(R-P- 2) – Lokalita používateľa a charakteristiky využívania sa musia chrániť pred neželaným odhalením.
(R-P- 3) – Musí sa umožniť ochrana dôvernosti identifikácie používateľských dát.
(R-P- 4) – V NGN sa musia podporovať anonymné komunikačné relácie, jednak v trvalom režime, alebo v dočasnom režime komunikácie pri volaní. V tom prípade identifikácia volajúcej strany sa nesmie prezentovať na strane volaného. Sieť, ku ktorej je volaná strana pripojená, je zodpovedná za spracovanie tejto služby.
(R-P- 5) – NGN musí podporiť špecifický prípad, ak volaná strana má právo zamedzenia (napríklad komunikačné relácie tiesňových volaní). Identifikácia volajúcej strany sa poskytuje k volanej strane nezávisle od toho, či je, alebo nie je táto komunikačná relácia anonymná.
(R-P- 7) – NGN musí podporovať pre prevádzkovateľa siete mechanizmy na garantovanie platnosti identifikácie používateľa prezentovanej v prichádzajúcom volaní k používateľovi, ak volanie je výlučne v tejto sieti prevádzkovateľa (napríklad volajúca strana a volaná strana sú účastníci jednej siete NGN).
(R-P- 8) – NGN musí poskytovať mechanizmy, ktoré umožnia prezentovať identifikáciu volajúceho v relácii, ak to nie je volajúcim zamedzené v relácii.
(R-AD- 2) – Poskytujú sa mechanizmy riadenia prístupu na zaistenie, že len oprávnení používatelia môžu pristúpiť k službe.
(R-AD- 4) – Na služby EMTEL sa musí poskytnúť dostupnosť a presná informácia o lokalite.
(R-AS- 1) – NGN v TISPAN musí poskytnúť smernice na vyhodnotenie a certifikáciu zariadení a systémov NGN.
(R-AS- 2) – Následky možného chybného použitia protokolov na bezpečnosť v NGN sa musia dokumentovať cez TVRA. To umožňuje používateľom odhadnúť potrebnú bezpečnosť pred využívaním daného protokolu.

5.5 Aplikačný server (AS)

Článok 5.5 obsahuje bezpečnostné požiadavky vzhľadom na aplikačné systémy.

POZNÁMKA. – Netvorí samostatný podsystém, ale bol začlenený na jednoduchšie vyhľadanie požiadaviek súvisiacich s AS.

Požiadavky na bezpečnosť
(R-AA- 1) – Prístup k sieťam, službám a aplikáciám NGN musí sa poskytnúť len oprávneným používateľom**.**
(R-AA- 4) – Na prístup k akejkoľvek službe IMS sa musí použiť ISIM, ale môžu sa povoliť výnimky pri tiesňových volaniach a starších rozvojových variantoch.
(R-AA- 8) – Dôležité špecifické informácie ISIM v NGN sa musia chrániť pred neoprávneným prístupom alebo zmenou.
(R-AA- 12) – Prenášané heslá sa musia vhodne chrániť, napríklad šifrovaním alebo inými spôsobmi.
(R-AA- 15) – Medzi UE a AS sa pred poskytnutím oprávnenia musí podporovať vzájomné overovanie totožnosti.
(R-AA- 16) – Musí sa podporovať aj architektúra založená na overení totožnosti zástupného servera. POZNÁMKA 1. – Účelom AP je oddeliť postup overenia totožnosti a logiku špecifickej aplikácie AS do rozličných logických jednotiek.
(R-AA- 17) – Medzi UE a AP sa musí podporovať vzájomné overovanie totožnosti.
(R-AA- 18) – AP musí rozhodnúť, či konkrétny účastník (napríklad UE) je oprávnený k prístupu ku konkrétnemu AS.

(R-AA- 19) – Ak sa použije AP, AS musí len autorizovať požiadavku prístupu k požadovanému prostriedku. POZNÁMKA 2. – AS nepotrebuje explicitne overiť totožnosť používateľa.
(R-SP- 1) – Sieť NGN podľa TISPAN musí byť logicky a fyzicky rozdelená na bezpečnostné domény umožňujúce oddelenie aplikácie (napríklad, IMS) a prenosu (napríklad ADSL a UMTS). Aj rozličníposkytovatelia podobných sietí (napríklad IMS) musia byť schopní prevádzkovať svoju vlastnú bezpečnostnú stratégiu.
(R-CD- 10) – Musí sa umožniť ochrana dôverných dát (ako sú informácia a potvrdenie o prítomnosti) pred útokmi (napríklad pred odpočúvaním, vniknutím a opakovanými útokmi).
(R-CD- 13) – Musí sa umožniť ochrana integrity signalizácie, riadiacej komunikácie a uložených dát.
(R-CD- 17) – Medzi UE a aplikačným serverom sa musí podporovať integrita dát.
(R-CD- 18) – Dôvernosť komunikácie sa musí dosiahnuť šifrovaním. Dôvernosť uložených dát sa musí dosiahnuť šifrovaním alebo kontrolou prístupu.
(R-CD- 19) – Dôvernosť signalizačných a riadiacich správ sa musí zaistiť, ak to požaduje aplikácia alebo prostredie, kde si to vyžaduje bezpečnostná stratégia. Mechanizmus musí umožniť výber použitého algoritmu.
(R-CD- 22) – Musí sa umožniť ochrana dôvernosti používateľských dát, ktoré uložil alebo spracúva prevádzkovateľ prevádzkovateľom.
(R-P- 2) – Lokalita používateľa a charakteristiky využívania sa musia chrániť pred neželaným odhalením.
(R-P- 3) – Musí sa umožniť ochrana dôvernosti používateľských identifikačných dát.
(R-P- 7) – NGN musí podporovať pre prevádzkovateľa siete mechanizmy na garantovanie platnosti identifikácie používateľa prezentovanej v prichádzajúcom volaní k používateľovi, ak volanie je výlučne v tejto sieti prevádzkovateľa (napríklad volajúca strana a volaná strana sú účastníci jednej siete NGN).
(R-P- 8) – NGN musí poskytovať mechanizmy, ktoré umožnia prezentovať identifikáciu volajúceho v relácii, ak to nie je volajúcim zamedzené v relácii.
(R-P- 9) – Súkromie prezentovanej informácie a potreba oprávnenia pred poskytovaním informácie o prezentácii sa musia dať konfigurovať používateľom (napríklad prítomnosť).
(R-P- 10) – Príkazca prezentácie musí byť vždy schopný kontrolovať, komu, ako dlho a čo (celá informácia alebo jej časť) sa poskytuje z prezentovanej informácie prezentácie, a príkazca dohľadu musí byť vždy schopný kontrolovať, komu, ako dlho a čo (celá informácia alebo jej časť) sa poskytuje z dohľadovej informácie dohľadu.
(R-P- 11) – Akékoľvek služby používajúce informáciu o prezentácii musia zaručiť súhlas s telekomunikačným tajomstvom pred uvoľnením informácie o prezentácii. Charakter služby neurčuje špecifické problémy využívania (napríklad, kde je uložený a ako je dohodnutý súhlas). Uvádza len požiadavky na administratívne riadenie súkromia.
(R-KM- 2) – UE a AS musia mať schopnosť obnoviť vopred zriadené bezpečné relácie.
(R-NF- 1) – Bezpečnostné protokoly NGN musia pracovať so spoločne využívanými firevalmi a musia pracovať v prostredí NAT/NATP.
(R-AD- 2) – Poskytujú sa mechanizmy riadenia prístupu na zaistenie, že len oprávnení používatelia môžu pristúpiť k službe.
(R-AS- 1) – NGN v TISPAN musí poskytnúť smernice na vyhodnotenie a certifikáciu zariadení a systémov NGN.
(R-AS- 2) – Následky možného chybného použitia protokolov na bezpečnosť v NGN sa musia dokumentovať cez TVRA. To umožňuje používateľom odhadnúť potrebnú bezpečnosť, pred využívaním daného protokolu.

Príloha A – Literatúra

ETSI TS 133 141 Universal Mobile Telecommunications System (UMTS). Presence service. Security (3GPP TS 33.141)

Príloha B – Bezpečnosť H.248

B.1 Základné údaje

Treba pripomenúť, že už existoval predpoklad, že sieť prevádzkovateľa predstavuje jednu zabezpečenú bezpečnostnú doménu. A teda akákoľvek komunikácia, ktorá zostáva v tejto sieti, je automaticky zabezpečená. Typický príklad takéhoto predpokladu je vytvorený v článku 4.5.1 v ES 283 002 [i.6].

V tejto architektúre sa predpokladá, že všetko v hranatých zátvorkách v súvisiacom diagrame je časťou domény prevádzkovateľa. Tento predpoklad sa potom použije na určenie, či tam nie je potreba použitia akýchkoľvek bezpečnostných mechanizmov na ochranu komunikácie medzi AGW a riadiacim podsystémom alebo RGW a riadiacim podsystémom.

B.2 Nároky na prijatie

Pri výstavbe NGN sa našiel prípad odmietajúci tento predpoklad. Realita NGN vedie k presvedčeniu, že sa nemôže viac zabezpečiť vnútorná sieť pre niekoľko príčin:

- Ako môže prevádzkovateľ v konkurenčnom, komerčnom svete zosilniť bytový sieťový priechod ako časti jeho domény? Realita bude, že účastníci budú používať mnoho rozličných sieťových priechodov so široko sa meniacou funkčnosťou.

- Prevádzkovatelia budujú sieť založenú na virtuálnych prístupových sieťových priechodoch umožňujúcich jednoduchý uvoľnený prístup k účastníckym vedeniam. V takých prípadoch, hoci účastník s uvoľneným prístupom bude fyzicky pripojený k sieti prevádzkovateľa, logicky bude časťou domény prevádzkovateľa uvoľneného prístupu, pripojený cez virtuálny prístupový sieťový priechod. Na volanie sa požaduje signalizácia k chrbticovej sieti a od chrbticovej siete prevádzkovateľa uvoľneného prístupu.

- Nedostatočne zabezpečený signalizačný protokol bude znamenať, že špeciálne služby, ako LI, budú menej spoľahlivé, ak sa implementujú do NGN v porovnaní so súčasnou situáciou.

- Pre príčiny znížených nákladov a zvýšenia pružnosti, NGN budú vybudované na transportných sieťach IP, ktoré sú otvorené a veľmi dobre známe možným útočníkom, v porovnaní s tradičnými telekomunikačnými sieťami so signalizáciou SS7, ktoré sa môžu brať do úvahy ako uzavreté domény.

- IPsec sa akceptoval ako štandardný spôsob ochrany prepojení v NGN s IP (v UK, právnou silou rozličných noriem NICC). Profil IPsec v NICC je viac komplexný, ako je navrhovaný v tejto technickej špecifikácii, pretože obsahuje ochranu dôvernosti pomocou šifrovania v súčinnosti s ochranou integrity.

- Dodatočne v čase životnosti súčasného NGN je zrejmé, že malí prevádzkovatelia (a možno niektorí väčší takisto) budú podporovať internet ako svoju chrbticovú sieť IP na svoje NGN.

Pre tieto príčiny je potom potreba overiť totožnosť komunikačných zariadení a tiež potreba zaistiť, že signály, ktoré vysielajú a prijímajú, nebudú napadnuté v trase.

Príklad je daný v súvislosti s riadiacou signalizáciou H.248. Časť normy H.248 definuje súbor požiadaviek na bezpečnosť signalizačného spojenia, ktoré sú založené na veľmi známych bezpečnostných normách IPsec z IETF.

IPsec je schopný použiť bezpečnostné služby šifrovania a integrity, ale navrhuje sa, že len ochrana integrity je reálne potrebná.

Použitie IPsec na ochranu H.248 požaduje, že komunikačné jednotky si vzájomne prísne overia totožnosť pred komunikáciou. Takisto je potrebné obnoviť relačné kľúče použité na ochranu signalizačných dát prenášaných v pravidelných intervaloch. Prirodzene, autori normy H.248 vynechali tieto dva dôležité aspekty zo svojich špecifikácií, vykonávajúci čisto odporúčania, že implementátor normy H.248 si bezpečnosť zaistí protokolom IKE na riadenie spojenia a certifikátov na overovanie totožnosti X.509.

Nedostatok spoľahlivých smerníc na riadenie spojení IPsec v normách H.248 vedie k rôznym riešeniam tohto problému produkovaným dodávateľmi zariadení, z ktorých nie všetky sú kompatibilné s IKE alebo skutočne akýmikoľvek inými riadiacimi riešeniami IPsec. Čistý výsledok je, že pre prevádzkovateľa snažiaceho sa vybudovať NGN nákupom zariadení od viacerých dodávateľov sa použitie IPsec na zabezpečenie spojení H.248 medzi viac dodávateľskými zariadeniami stáva extrémne ťažké, ak nie nemožné na riadenie použitia medzi dvomi alebo viacerými vzájomne nekompatibilnými riadiacimi mechanizmami.

Ukazuje sa niekoľko možných spôsobov vybudovania ochrany integrity IPsec do H.248:

- požiadavky na takú ochranu by mohli formulovať a venovať jej pozornosť vlastníci normy H.248 to má byť cieľom definovania štandardného profilu IPsec na ochranu H.248 a na vyplnenie medzier v súčasnej verzii normy

- požiadavky na takú ochranu by sa mohli formulovať v TISPAN a navrhnúť ako doplnok súčasného dokumentu smerujúci k normatívnemu textu na bezpečnosť v H.248 (verzia 2) 7.1 R-MGF Context a 7.2 A-MGF Context v TS 187 005 [i.7] architektúra bezpečnosti, verzia 2.

V tom prípade požiadavky by mali obsahovať riešenie štandardného riadenia IPsec. Existujú dve možnosti:

- Riešenie podľa TS 133 210 [3] a TS 133 310 [i.8], ale malo by sa rešpektovať, že riadenie certifikátu bude mať stupnicu podľa usporiadania použitého v doménach prevádzkovateľov a medzi malým počtom prevádzkovateľov s existujúcimi zmluvami o roamingu, až do usporiadania s veľkým počtom RGW.

- Riešenia vhodnejšie s veľkým počtom RGW založené na EAP-AKA a certifikácii siete sú sa špecifikujú v TS 133 234 [i.9] (WLAN 3GPP IP Access).

B.3 Možné nevýhody

IPsec je ťažko konfigurovať – pridáva extra súbor príležitostí pre problémy pri výstavbe siete. Použitie štandardného profilu IPsec na zabezpečenie H.248 v sieti prevádzkovateľa bude požadovať určitý rozvoj akéhokoľvek monitorovania signalizácie, ktoré sa stáva schopné skúšať používateľské dáta paketov overovania totožnosti IPsec. Súčasne také monitory majú miesto v sieti a pasívne monitorujú prechádzajúcu signalizačnú prevádzku. Táto požiadavka neznamená, že signalizačné monitory sa stávajú časťou siete IPsec, pretože používateľské dáta paketu chrániaceho integritu IPsec sú prázdne. Nijaké vedomosti o kľúči ochrany integrity IPsec sa nepožadujú, aby sa dekódovali používateľské údaje signalizačného paketu.

V minulosti mnohí dodávatelia zariadení a ich účastníci sa bránili použiť IPsec, pretože údajne mohli nepriaznivo ovplyvniť výkonnosť ich zariadení. Teraz už neplatí s modernou výpočtovou technikou, či je perfektne možné implementovať do zariadenia, ako sú mobilné náhlavné súpravy, úplne automatické riešenie IPsec bez akýchkoľvek problémov, ako je dodatočné oneskorenie.

Príloha C – Bezpečnostné domény v NGN

POZNÁMKA. – Výraz „zabezpečený“ nie je definovaný v norme ISO 27000 [i.10] Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.

C.1 Definícia zabezpečenia NGN – analýza

Norma ISO 15408-1 nepriamo definuje zabezpečenie, ale nedefinuje zabezpečený kanál a zabezpečenú trasu. Norma ISO 15408-2 definuje funkčné schopnosti (použité vo vrstve funkčnej požiadavky metóda bezpečnostných požiadaviek TISPAN v TR 187 011 [i.11]), ktorá sa môže použiť na zjemnenie zabezpečenia v NGN.

Zabezpečený kanál (angl. **trusted channel):** prostriedky, ktorými TSF a vzdialený zabezpečený produkt IT môže komunikovať s potrebnou dôvernosťou a podporovať TSP.

Zabezpečená trasa (angl. **trusted path)**: prostriedky ktorými používateľ a TSF môže komunikovať s potrebnou dôvernosťou a podporovať TSP.

S NGN sa predpokladá, že TSF je NGN a že TSP sú stratégie požadované na zaručenie bezpečnosti NGN.

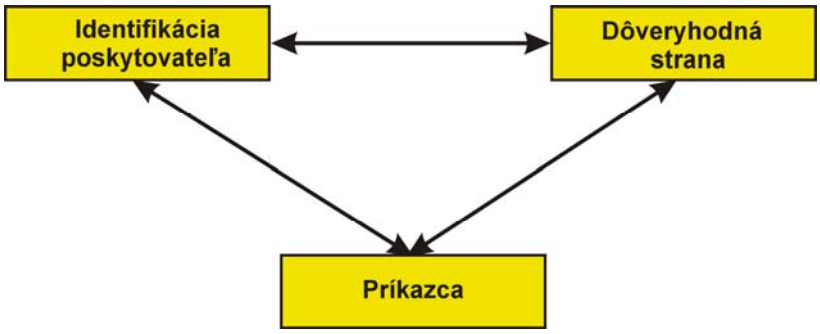
V NGN zabezpečenie opisuje vzťah medzi jednotkami, kde je overovanie výroku identifikácie a autorizácie medzi jednotkami.

Ako sa uvádza v TR 187 010 [i.12], spôsob identifikácie pozostáva z troch prvkov:

- Príkazca:
  - často je to synonymum pre koncového používateľa a v telekomunikačných protokoloch chápaný ako elektronická alebo digitálna reprezentácia človeka ako koncového používateľa.

POZNÁMKA. – V riadení účastníka v NGN príkazca môže byť človek skôr ako jeho reprezentácia ako koncového používateľa.

- Identifikácia poskytovateľa služby (IdP):
  - základná úloha IdP v IdM je overiť totožnosť príkazcu a poskytnúť výrok o overení jeho totožnosti pre dôveryhodnú stranu.
- Dôveryhodná strana (RP)
  - RP poskytuje službu príkazcovi; z tejto strany príkazca si môže overiť totožnosť k RP, ale RP sa takisto chce spoliehať na výrok poskytovaný IdP.



Obrázok C.1 – Pravidlá (alebo jednotky) na overovanie totožnosti, SSO a varianty identifikácie federácie (z TR 187 010)

Vytvorenie zabezpečenia požaduje, aby dôveryhodná strana akceptovala výrok identifikácie poskytovaný poskytovateľom identifikácie pred ponúkaním služby príkazcovi.

V prípadoch, kde RP je v oddelenej NGN od IdP, napríklad, ak NGCN je komunikujúca s NGN, kde NGN pracuje ako RP a NGCN ako IdP, výrok identifikácie sa môže dosiahnuť pomocou mechanizmov overenia totožnosti, kde RP a IdP spolupracujú na úplnom overení totožnosti (napríklad overovanie totožnosti vykonáva záväzne RP založené na výrokoch príkazcu).

C.2 Požiadavky na vytvorenie zabezpečeného kanála

Nasledujúci model s definíciou požiadaviek v TR 187 011 vytvára ďalej uvedené výroky.

C.2.1 Funkčné požiadavky na bezpečnosť zabezpečeného kanála v NGN

Funkčné požiadavky sú určené ako stupňovanie funkčných vlastností uvedené v norme ISO 15408-2 [i.3].

NGN poskytuje komunikačný kanál medzi sebou a vzdialenou NGN/NGCN, ktorý sa logicky odlišuje od iných komunikačných kanálov a poskytuje zaistenú identifikáciu jej koncových bodov a ochranu dátového kanála od zmien alebo odhalenia (z normy ISO 15408-2 FTP_ITC.1.1 [i.3]).

NGN dovoľuje jednotke CSCF NGN iniciovať komunikáciu cez zabezpečený kanál (z normy ISO 15408-2 FTP_ITC.1.1 [i.3]).

NGN dovoľuje jednotke CSCF NGCN iniciovať komunikáciu cez zabezpečený kanál (z normy ISO 15408-2 FTP_ITC.1.1 [i.3]).

C.3 Existujúce vlastnosti NGN

Existujúce vlastnosti NGN sa uvádzajú v normách RFC 3324 [i.4] Short Term Requirements for Network Asserted Identity a RFC 3325 [i.5]: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.

P-Asserted Identity (PAI) sa používa na indikáciu, že zástupný server SIP berie do úvahy kroky na schválenie identifikácie obsiahnutej v záhlaví PAI. V mapovaní podľa modelu

identifikácie v kapitole C.1 zástupný server SIP pracuje ako dôveryhodná strana a prenáša túto informáciu na prijatie SIP-UA, ktorý takisto pracuje ako dôveryhodná strana.

Výroky v RFC 3324 [i.4] sú, že táto PAI, ak je prítomná v správach, indikuje toto:

- INVITE – volajúci používateľ,
- 180 Response – vyzváňanie používateľa,
- 200 OK – používateľ sa prihlásil.

Správanie zástupného servera SIP a SIP UAS je určené schopnosťou zástupného servera SIP UAS na identifikáciu zabezpečenej domény. Špecifikácia PAI neudáva, ako je zabezpečené zaistenie pri PAI.

História

História dokumentu		
V2.1.5	Október 2008	Publikovanie