Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Conforme à l'original produit,
Début du texte, page suivante.

BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°8 du 13 février 2009

PARTIE PERMANENTE
Administration Centrale

Texte n°1

DIRECTIVE N° 7/DEF/DGSIC
portant sur la téléphonie sur le protocole internet.

Du *13 janvier 2009*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 7/DEF/DGSIC portant sur la téléphonie sur le protocole internet.

Du 13 janvier 2009

NOR D E F M 0 9 5 0 0 3 7 X

Références :

Ordonnance n° 2005-1516 du 8 décembre 2005 (JO n° 286 du 9 décembre 2005, texte n° 9 ; BOC, p. 8645. ; BOEM 120-0.3.1).
Décret n° 2006-497 du 2 mai 2006 (n.i. BO ; JO n° 103 du 3 mai 2006, texte n° 9 ; JO/135/2006. ; BOEM 160.1).

Pièce(s) Jointe(s) :

Deux annexes.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°8 du 13 février 2009, texte 1.

---

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive définit la politique à mettre en œuvre avant le déploiement d'un service de téléphonie sur le protocole internet (ToIP) par les organismes du ministère de la défense. Elle fournit les critères de décision pour l'acquisition, la réalisation et la mise en œuvre d'un service de ToIP.

Par la nature du service rendu, la téléphonie, étendue fonctionnellement ou non, est un service sensible et critique, voire vital pour certains organismes, les attentes en matière de qualité et de sécurité (disponibilité, confidentialité, intégrité et authentification) sont très fortes.

Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

Elle décline la directive n° 1/DEF/DGSIC sur les logiciels [DGSIC001] du ministère de la défense.

Elle tient compte du projet de référentiel général d'interopérabilité [RGI] dans sa version provisoire V0.98 de juin 2007 prescrit par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives et du projet de référentiel général de sécurité [RGS] dans sa version provisoire V0.96 du 31 mai 2007.

1.2. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au RGI* et à la [RFC 2119] :

- OBLIGATOIRE : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- RECOMMANDÉ : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- DÉCONSEILLÉ : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- INTERDIT : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Modalités d'application.**

Cette directive est applicable aux systèmes d'information et de communication (SIC) non classifiés de défense support d'un service de ToIP et à tous leurs composants, notamment leurs éléments actifs. Elle concerne les aspects suivants : organisation, technique, sécurité, exploitation, fonctionnel et maintenance. Elle fait partie de la politique de sécurité du SIC, support d'un service de ToIP, qui doit être formellement redéfinie suivant les modalités en vigueur.

Les règles de la présente directive définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure de projet de téléphonie sur IP mis en œuvre sur un réseau au protocole IP*.

Cette directive sera appliquée dans un délai de trois ans pour les réseaux ayant fait ou faisant actuellement l'objet d'un portage en ToIP et dès la conception pour ceux nécessitant obligatoirement des rénovations orientées vers une solution ToIP, en avance de phase de tout réseau support.

1.4. **Gestion des dérogations pour les projets.**

Elles sont instruites par la CMTSIC* et font l'objet d'une approbation par le directeur de la DGSIC.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

- [CPCE] - Code des postes et des communications électroniques (1).

- [Loi 1978] - Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

- [Loi1991] - Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

- [IGI 1300] - Instruction générale interministérielle sur la protection du secret de la Défense nationale n° 1300 SGDN/PSE/SSD (1) du 25 août 2003.

- [IGI 901] - Recommandation n° 901/DISSI/SCSSI du 2 mars 1994.

- [CCI] - Recommandations nationales du Cadre Commun d'Interopérabilité.

- [RGI] - Référentiel Général d'Interopérabilité.

- [RGS] - Référentiel Général de Sécurité.

- [PRIS] - Politique de Référencement Intersectoriel de Sécurité.

- [PSSI] - Instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'information du ministère de la défense.

- [DGSIC001] - Directive n° 1/DEF/DGSIC du 17 octobre 2006 portant sur les logiciels du ministère de la défense.

- [DGSIC002] - Directive n° 2/DEF/DGSIC du 9 mars 2007 modifiée portant sur le système d'annuaires (SA) du ministère de la défense.

- [DGSIC003] - Directive n° 3/DEF/DGSIC du 8 janvier 2008 définissant les règles de la messagerie électronique.

- [OSCAR] - Directive d'orientation pour la sécurisation des interconnexions et des architectures de réseaux « OSCAR » diffusée par la note n° 178/DEF/SEC.DIR.SIC du 4 mai 2001 (1).

- [IM8192] - Instruction n° 8192/DEF/SEC/DIR/SIC du 30 juin 2003 relative aux modalités d'accès, de raccordement et d'utilisation des réseaux externes au ministère de la défense.

- [EMA1233] - Note n° 1233/DEF/EMA/PI/-- du 2 juin 2005 (1) (version 2.1) relative à la politique d'interconnexion des réseaux IP de la défense.

- [PSI1] - Politique de sécurité de l'Intradef version 1.0 du 4 décembre 2000 diffusée par la note n° 2448/DEF/EMA/TSIC/4 du 6 décembre 2000 (1).

- [DIRSIC365] - Note n° 365/DEF/SEC/DIR/SIC du 25 juillet 2002 (1) relative aux dangers de l'utilisation des réseaux sans fil.

- [DGSIC259] - Note n° 259/DEF/DGSIC du 15 juin 2006 (1) relative aux spécifications de sécurisation et régime dérogatoire pour les nouvelles technologies.

2.2. **Normes et standards applicables pour la téléphonie sur le protocole internet.**

2.2.1. ***Définitions.***

- [RFC 2119] - Mots-clés pour niveaux d'obligation.

2.2.2. ***Signalisation « session initiation protocol ».***

- [RFC 2352] - Extended facsimile using internet mail.

- [RFC 3261] - SIP : Session Initiation Protocol.

- [RFC 3262] - Reliability of provisional responses in Session Initiation Protocol (SIP).

- [RFC 3263] - Session Initiation Protocol (SIP) locating SIP servers.

- [RFC 3264] - An offer/answer model with Session Description Protocol (SDP).

- [RFC 3265] - Session Initiation Protocol (SIP) - specific event notification (met à jour le RFC 3261).

- [RFC 3312] - Integration of resource management and Session Initiation Protocol (SIP).

- [RFC 3319] - Dynamic Host Configuration Protocol (DHCPv6) options for Session Initiation Protocol (SIP) servers.

- [RFC 3327] - Session Initiation Protocol (SIP) extension header field for registering non-adjacent contacts.

- [RFC 3329] - Security mechanism agreement for the Session Initiation Protocol (SIP).

- [RFC 3362] - Real-time facsimile (T.38) - image/t38 MIME Sub-type registration.

- [RFC 3398] - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping.

- [RFC 3428] - Session Initiation Protocol (SIP) extension.

- [RFC 3487] - Requirements for resource priority mechanisms for the Session Initiation Protocol (SIP).

- [RFC 3578] - Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) overlap signalling to the Session Initiation Protocol (SIP).

- [RFC 3581] - An extension for the Session Initiation Protocol (SIP) for symmetric response routing.

- [RFC 3666] - Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) call flows.

- [RFC 3761] - The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) application (ENUM).

- [RFC 3762] - Telephone Number Mapping (ENUM) service registration for H.323.

- [RFC 3853] - S/MIME Advanced Encryption Standard (AES) requirement for the Session Initiation Protocol (SIP).

- [RFC 3856] - A presence event package for the Session Initiation Protocol (SIP).

- [RFC 3893] - Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) format.

- [RFC 3953] - Telephone Number Mapping (ENUM) service registration for presence services.

- [RFC 3959] - The early session disposition type for the Session Initiation Protocol (SIP).

- [RFC 3960] - Early media and ringing tone generation in the Session Initiation Protocol (SIP).

- [RFC 4032] - Update to the Session Initiation Protocol (SIP) preconditions framework.

- [RFC 4142] - Full-mode Fax Profile for Internet Mail (FFPIM).

- [RFC 4143] - Facsimile Using Internet Mail (IFAX) service of ENUM.

- [RFC 4320] - Actions addressing identified issues with the Session Initiation Protocol's (SIP) non-INVITE transaction (met à jour le RFC 3261).

- [RFC 4411] - Extending the Session Initiation Protocol (SIP) reason header for pre-emption events.

- [RFC 4414] - An ENUM registry type for the Internet Registry Information Service (IRIS).

- [RFC 4458] - Session Initiation Protocol (SIP) URIs for applications such as Voicemail and Interactive Voice Response (IVR).

- [RFC 4474] - Enhancements for authenticated identity management in the Session Initiation Protocol (SIP).

- [RFC 4479] - A Data model for presence.

- [RFC 4497] - Internetworking between the Session Initiation Protocol (SIP) and QSIG.

- [RFC 4740] - Diameter Session Initiation Protocol (SIP) application.

- [RFC 4759] - The ENUM Dip indicator parameter for the tel URI.

- [RFC 4769] - IANA Registration for an Enum service containing Public Switched Telephone Network (PSTN).

- [RFC 4780] - Management Information Base for the Session Initiation Protocol (SIP).

- [RFC 4825] - The Extensible Markup Language (XML) Configuration Access Protocol (XCAP).

- [RFC 4826] - Extensible Markup Language (XML) formats for representing resource lists.

- [RFC 4827] - An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) usage for manipulating presence document contents.

- [RFC 4916] - Connected Identity in the Session Initiation Protocol (SIP).

- [RFC 5367] - Subscriptions to Request-Contained resource Lists in the Session Initiation Protocol (SIP).

2.2.3. ***Signalisation H323*.***

- [H.225.0] - Call signalling protocols and media stream packetization for packet-based multimedia communication systems.

- [H.235.0] - H.323 Security : Framework for security in H series (H.323 and other H.245 based) multimedia systems.

- [H.235.1] - H.323 Security : Basic security profile.

- [H.235.2] - H.323 Security : Signature security profile.

- [H.235.3] - H.323 Security : Hybrid security profile.

- [H.235.4] - H.323 Security : Direct and selective routed call security.

- [H.235.5] - H.323 Security : Framework for secure authentication in RAS using weak shared secrets.

- [H.235.6] - H.323 Security : Voice encryption profile with native H.235/H.245 key management.

- [H.235.7] - H.323 Security : Usage of MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235.

- [H.235.8] - H.323 Security : Security gateway support for H.323.

- [H 245] - Control protocol for multimedia communication.

- [H.323] - Packet-based multimedia communications systems.

- [H.350] - Directory services architecture for multimedia conferencing.

- [H.350.1] - Directory services architecture for H.323.

- [H.350.2] - Directory services for H.235.

- [H.350.3] - Directory service architecture for H.320.

- [H.350.4] - Directory services architecture for SIP.

- [H.350.5] - Directory services architecture for non-standard protocols.

- [H.350.6] - Directory services architecture for call forwarding and preferences.

- [H.350.7] - Directory services architecture for XMPP.

- [H.450.1] - Generic functional protocol for the support of supplementary services in H.323.

- [H.450.2] - Call transfer supplementary service for H.323.

- [H.450.3] - Call diversion supplementary service for H.323.

- [H.450.4] - Call hold supplementary service for H.323.

- [H.450.5] - Call park and call pickup supplementary services for H.323 + Erratum (May 2000).

- [H.450.6] - Call waiting supplementary services for H.323.

- [H.450.7] - Message waiting indication supplementary service for H.323.

- [H.450.8] - Name identification supplementary services for H.323.

- [H.450.9] - Call completion supplementary services for H.323.

- [H.450.10] - Call offering supplementary service for H.323.

- [H.450.11] - Call intrusion supplementary service for H.323

- [H.450.12] - Common Information additional Network Feature for H.323.

- [H.460.1] - Guidelines for the use of the generic extensible framework.

- [H.460.2] - Number Portability internetworking between H.323 and SCN networks.

- [H.460.3] - Circuit maps within H.323 systems.

- [H.460.4] - Call priority designation and country/international network of call identification for H.323 priority calls.

- [H.460.5] - H.225.0 transport of multiple Q.931 information elements of the same type.

- [H.460.6] - Extended Fast Connect feature.

- [H.460.7] - Digit maps within H.323 systems.

- [H.460.8] - Querying for alternate routes within H.323 systems.

- [H.460.9] - Support for online QoS-monitoring reporting within H.323 systems.

- [H.460.10] - Call party category within H.323 systems.

- [H.460.11] - Delayed call establishment within H.323 systems.

- [H.460.12] - Glare control indicator within H.323 systems.

- [H.460.13] - Called user release control.

- [H.460.14] - Support for Multi-Level Precedence and Preemption (MLPP) within H.323 systems.

- [H.460.15] - Call signaling transport channel suspension and redirection within H.323 systems.

- [H.460.16] - Multiple message released sequence capability.

- [H.460.17] - Using H.225.0 call signaling connection as transport for H.323 RAS messages.

- [H.460.18] - Traversal of H.323 media across network address translators and firewalls.

- [H.460.19] - Traversal of H.323 media across network address translators and firewalls.

- [H.460.20] - Location number within H.323 systems.

- [H.460.21] - Message broadcast for H.323 systems.

- [H.460.22] - Negotiation of security protocols to protect H.225.0 Call Signaling Messages.

- [H.501] - Protocol for mobility management and intra/inter-domain communication in multimedia systems.

- [H.510] - Mobility for H.323 multimedia systems and services.

- [H.530] - Symmetric security procedures for H.323 mobility in H.510.

- [T.37] - Procedures for the transfer of facsimile data via store-and-forward on the Internet.

- [T.38] - Procedures for real-time Group 3 facsimile communication over IP network.

- [T.122] - Multipoint communication service - Service definition.

- [T.124] - Generic conference control.

- [T.125] - Multipoint Communication Service Protocol (MCS).

- [T.126] - Multipoint still image and annotation protocol.

- [T.127] - Multipoint binary file transfer protocol.

- [T.128] - Multipoint application sharing.

- [X.224] - Information technology - Open Systems Interconnections - Protocol for providing the connection-mode transport service.

2.2.4. ***Encodage media voix.***

- [G.711] - Pulse Code Manipulation (PCM) of voice frequencies.

- [G.723.1] - Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s.

- [G.728] - Coding of speech at 16kbit/s using low-delay code excited linear prediction.

- [G.729] - Coding of speech at 8 kbit/s using conjugate-structure algebraic code-excited linear prediction (CS-ACELP).

- [G.722] - 7 KHz audio-coding within 64 kbit/s.

- [G.726] - 40, 32, 24, 16 kbit/s Adaptative Differential Pulse Code Modulation (ADPCM).

- [G.727] - 5-, 4-, 3- and 2- bit/sample embedded adaptive differential pulse code modulation (ADPCM).

- [RFC 3951] - Internet Low Bit Rate Codec (iLBC).

2.2.5. ***Encodage video.***

- [H.261] - Video codec for audiovisual services at p x 64 kbit/s.

- [H.262] - Information technology - Generic coding of moving pictures and associated information: Video.

- [H.263] - Video coding for low bit rate communication.

- [H.264] - Advanced video codec for generic audiovisual services.

- [H.264.1] - Conformance specification for H.264 advanced video coding.

- [H.264.2] - Reference software for H.264 advanced video coding.

2.2.6. ***Annulation d'écho.***

- [G.108.2] - Transmission planning aspects of echo cancellers.

- [G.164] - Echo suppressors.

- [G.165] - Echo cancellers.

- [G.168] - Digital network echo cancellers.

2.2.7. ***Contrôle des passerelles « media gateway control protocol ».***

- [RFC 3435] - Media Gateway Control Protocol (MGCP) version 1.0.

- [RFC 3660] - Basic Media Gateway Control Protocol (MGCP) Packages.

- [RFC 3661] - Media Gateway Control Protocol (MGCP) return code usage (met à jour RFC 3435).

2.2.8. ***Contrôle des passerelles MEGACO*/H.248*.***

- [RFC 2805] - Media Gateway Control Protocol Architecture and Requirements.

- [RFC 3525] - Megaco Protocol version 1.

- [H.248.1] - Gateway control protocol : Version 3.

- [H.248.2] - Gateway control protocol : Facsimile, text conversation and call discrimination packages.

- [H.248.3] - Gateway control protocol : User interface elements and actions packages.

- [H.248.4] - Gateway control protocol : Transport over Stream Control Transmission Protocol (SCTP).

- [H.248.5] - Gateway control protocol : Transport over ATM.

- [H.248.6] - Gateway control protocol : Dynamic tone definition package.

- [H.248.7] - Gateway control protocol : Generic Announcement package.

- [H.248.8] - Gateway control protocol : Error code and service change reason description.

- [H.248.9] - Gateway control protocol : Advanced media server package.

- [H.248.10] - Gateway control protocol : Media gateway resource congestion handling package.

- [H.248.11] - Gateway control protocol : Media gateway overload control package.

- [H.248.12] - Gateway control protocol : H.248.1 packages for H.323 and H.324 internetworking.

- [H.248.13] - Gateway control protocol : Quality Alert Ceasing package.

- [H.248.14] - Gateway control protocol : Inactivity timer package.

- [H.248.15] - Gateway control protocol : SDP H.248 package attribute.

- [H.248.16] - Gateway control protocol : Enhanced digit collection packages and procedures.

- [H.248.17] - Gateway control protocol : Line test packages.

- [H.248.18] - Gateway control protocol : Package for support of multiple profile.

- [H.248.19] - Gateway control protocol : Decomposed multipoint control unit, audio, video and data conferencing packages.

- [H.248.20] - Gateway control protocol : The use of local and remote descriptors with H.221 and H.223 multiplexing.

- [H.248.21] - Gateway control protocol : Semi-permanent connection handling package.

- [H.248.22] - Gateway control protocol : Shared Risk Group package.

- [H.248.23] - Gateway control protocol : Enhanced Alerting packages.

- [H.248.24] - Gateway control protocol : Multi-frequency tone generation and detection packages.

- [H.248.25] - Gateway control protocol : Basic CAS packages.

- [H.248.26] - Gateway control protocol : Enhanced analog lines package.

- [H.248.27] - Gateway control protocol : Supplemental tones package.

- [H.248.28] - Gateway control protocol : International CAS package.

- [H.248.29] - Gateway control protocol : International CAS compelled register signaling packages.

- [H.248.30] - Gateway control protocol : RTCP extended performance metrics packages.

- [H.248.31] - Gateway control protocol : Adaptive jitter buffer package.

- [H.248.32] - Gateway control protocol : Detailed congestion reporting package.

- [H.248.33] - Gateway control protocol : PCM frame spare bit packer.

- [H.248.34] - Gateway control protocol : Stimulus analogue lines package.

- [H.248.35] - Gateway control protocol : Coin package.

- [H.248.36] - Gateway control protocol : Hanging Termination Detection package.

- [H.248.37] - Gateway control protocol : IP NAPT traversal package.

- [H.248.38] - Gateway control protocol : Base context package.

- [H.248.39] -Gateway control protocol : H.248 SDP parameter identification and wildcarding.

- [H.248.40] - Gateway control protocol : Application Data Inactivity Detection Package.

- [H.248.41] - Gateway control protocol : IP domain connection package.

- [H.248.42] - Gateway control protocol : DCME internetworking package.

- [H.248.44] - Gateway control protocol : Multi-level precedence and pre-emption package.

- [H.248.45] - Gateway control protocol : MGC information package.

- [H.248.46] - Gateway control protocol : Connection Capability Control package.

- [H.248.47] - Gateway control protocol : Statistic conditional reporting package.

2.2.9. ***Transport média RTP/RTCP.***

- [RFC 3550] - RTP : a Transport Protocol for Real-Time applications.

- [RFC 4588] - RTP retransmission payload format.

- [RFC 4585] - Extended RTP profile for Real-time Transport Control Protocol (RTCP)-based feedback (RTP/AVPF).

- [RFC 4571] - Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) packets over connection-oriented transport.

- [RFC 3611] - RTP control protocol extended reports (RTCP XR).

- [RFC 3605] - Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP).

- [RFC 3556] - session description Protocol (SDP) bandwidth modifiers for RTP Control Protocol (RTCP) bandwidth.

- [RFC 3640] - Payload format for transport of MPEG-4 elementary streams.

- [RFC 3551] - RTP profile for audio and video conferences with minimal control.

- [RFC 4733] - RTP Payload for DTMF digits, telephony tones and telephony signals.

- [RFC 4734] - Definition of events for modem, fax and text telephony signals.

- [RFC 5244] - Definition of Events for Channel-Oriented Telephony Signalling.

2.2.10. ***Transport média SRTP* et SRTCP*.***

- [RFC 3711] - The Secure Real-time Transport Protocol (SRTP).

2.2.11. ***Transport média RTSP*.***

- [RFC 2326] - Real Time Streaming Protocol (RTSP).

- [RFC 4567] - Key management extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP).

2.2.12. ***Transport média SCTP.***

- [RFC 4960] - Stream Control Transmission Protocol.

- [RFC 3331] - Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User adaptation layer.

- [RFC 3436] - Transport Layer Security over Stream Control Transmission Protocol.

- [RFC 3554] - On the use of Stream Control transmission Protocol (SCTP) with IPsec.

- [RFC 3758] - Stream control Transmission Protocol (SCTP) partial reliability extension.

- [RFC 3807] - V5.2 user adaptation layer (V5UA).

- [RFC 3868] - Signaling Connection Control part user adaptation layer (SUA).

- [RFC 3873] - Stream Control transmission Protocol (SCTP) Management Information Base (MIB).

- [RFC 4168] - The Stream Control transmission Protocol (SCTP) as a transport for the Session Initiation Protocol (SIP).

- [RFC 4233] - Integrated Services Digital Network (ISDN) Q.921 - user adaptation layer.

- [RFC 4666] - Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - user adaptation layer (M3UA).

- [RFC 4820] - Padding chunk and parameter for the Stream Control transmission Protocol (SCTP).

- [RFC 5133] - Terminal Endpoint Identifier (TEI) Query Request Number Change.

2.3. **Normes et standards applicables pour les services support.**

2.3.1. ***Normes et standards applicables pour la sécurisation du transport TCP : TLS*.***

- [RFC 3436] - Transport Layer Security over Stream Control Transmission Protocol.

- [RFC 4572] - Connection-oriented media transport over the Transport Layer Security (TLS). protocol in the Session Description Protocol (SDP).

2.4. **Normes et standards applicables pour l'infrastructure réseau.**

- [802.3af] - DTE power via MDI.

- [802.1p] - Traffic class expediting and dynamic multicast filtering (published in 802.1D-1998).

- [802.1q] - Virtual LANs.

- [802.1x] - Port based network access control.

- [802.1ab] - Station and Media Access Control Connectivity Discovery.

3. DOMAINE COUVERT ET EMPLOI.

La directive vise à définir des mécanismes permettant la mise en œuvre d'un système de téléphonie étendu (voix, vidéo, conférence, présence) ou non, ainsi que des liaisons à des services connexes (gestion, administration et contrôle). Elle comprend aussi l'organisation humaine nécessaire au bon fonctionnement de ce système.

3.1. **Services attendus.**

La ToIP* doit permettre la communication en temps réel* sous différentes formes (audio, vidéo, écrit) entre plusieurs personnes internes ou externes au ministère de la défense et éventuellement étendues aux fonctionnalités présence, conférences audio et visiophonie, messagerie instantanée, et unification avec le courrier électronique.

3.2. **Périmètre et limites.**

Le périmètre de la présente directive concerne les règles, architectures et mécanismes qui permettent la communication entre des personnes ainsi que certains des éléments de la politique de sécurité. Le domaine couvert concerne la *téléphonie dite administrative**. La messagerie instantanée et la présence ne sont pas traitées au sein de ce document.

3.3. **Interopérabilité.**

3.3.1. ***Avec les applications.***

La ToIP devra s'interfacer avec les services et applications en utilisant des normes et protocoles standardisés tels que LDAP* pour l'annuaire, NTP* pour la synchronisation des horloges ou XMPP* pour la messagerie instantanée et la gestion de présence, selon les directives en vigueur.

*3.3.2. **Avec les systèmes de téléphonie sur le protocole internet.***

Les règles énoncées ci-dessous doivent permettre d'assurer l'interchangeabilité des systèmes de ToIP* entre eux, ainsi qu'avec les systèmes existants et le monde extérieur. En ce qui concerne les nouveaux systèmes, l'interopérabilité n'est jamais acquise elle doit donc être OBLIGATOIREMENT testée sur plateforme représentative du système dans son ensemble, systématiquement recettée (VABF) et contrôlée (VSR).

4. LES RÈGLES.

Les règles sont regroupées et énoncées suivant les aspects technique (RT), organisationnel (RO) et sémantique (RS). Elles sont numérotées séquentiellement par catégorie.

4.1. **Règles techniques.**

*4.1.1. **Transport de la conversation.***

- RT 01 : il est OBLIGATOIRE de disposer d'un réseau support IP gérant la qualité de service (la QoS*) pour assurer au profit de la téléphonie une gestion optimale de la bande passante.

- RT 02 : il est RECOMMANDÉ de ne pas dépasser 60 p.100 de charge moyenne sur les équipements actifs afin de se prémunir efficacement des effets de saturation et de maîtriser la gigue*.

*4.1.2. **Signalisation.***

- RT 03 : il est RECOMMANDÉ d'utiliser SIP* v2.

- RT 04 : afin d'assurer la portabilité des terminaux, il est RECOMMANDÉ d'utiliser des téléphones SIP standard.

*4.1.3. **Administration.***

- RT 05 : il est RECOMMANDÉ de protéger les flux d'administration en confidentialité, intégrité et d'avoir une authentification mutuelle entre un administrateur et l'équipement administré.

- RT 06 : il est RECOMMANDÉ d'utiliser les protocoles TLS ou SSH v2 pour l'administration à distance des serveurs et des équipements de téléphonie.

*4.1.4. **Sécurité.***

Cloisonnement :

- RT 07 : il est OBLIGATOIRE de cloisonner le réseau de ToIP par rapport au réseau de données (dit informatique) soit par séparation physique des réseaux ou, à défaut, par séparation logique au moyen de réseaux virtuels locaux (VLAN).

- RT 08 : il est RECOMMANDÉ de séparer les équipements ayant des fonctionnalités et des besoins de sécurité différents en autant de réseaux virtuels locaux (VLAN, IEEE 802.1Q) que de fonctions, à savoir les serveurs de ToIP, les téléphones IP, les passerelles RTC*, les équipements d'administration en définissant des politiques de protections spécifiques en fonction de la sensibilité et des besoins de sécurité des équipements et des informations qu'ils portent.

- RT 09 : il est OBLIGATOIRE de cloisonner les données d'administration des équipements vis-à-vis des flux de données, soit par séparation physique ou, à défaut, par séparation logique au moyen de réseaux virtuels locaux (VLAN) spécifiques.

- RT 10 : il est OBLIGATOIRE que les services de réseaux DNS, DHCP et NTP soient propres à la téléphonie (il ne doit pas y avoir de partage avec les services du réseau de données informatiques) y compris pendant les seules phases de pré-déploiement et configuration.

Services support :

- RT 11 : si DHCP est utilisé, il est OBLIGATOIRE que l'association adresse MAC* et adresse IP* soit fixe et que des mesures anti-spoofing* soient mises en œuvre.

- RT 12 : il est OBLIGATOIRE que seuls les *équipements légitimes** aient le droit de se connecter au réseau de téléphonie.

- RT 13 : il est RECOMMANDÉ que les fichiers de configuration des téléphones soient chiffrés et signés à l'aide d'un dispositif cryptographique.

- RT 14 : dans le cas où la RT 12 ne peut être appliquée, il est RECOMMANDÉ d'utiliser SFTP* (SSH File Transfer Protocol) pour le téléchargement des fichiers de configuration des téléphones.

- RT 15 : il est OBLIGATOIRE que le service de téléphonie utilise l'heure et la date de référence du ministère.

Sécurisation des commutateurs Ethernet :

- RT 16 : il est OBLIGATOIRE de limiter le nombre d'adresses MAC à 3 par port*.

- RT 17 : il est OBLIGATOIRE que les ports des commutateurs Ethernet inutilisés soient verrouillés (il est impossible de se connecter au réseau sans intervention d'un administrateur). Dans le cas de commutateurs intégrés aux téléphone et permettant la connexion d'un ou plusieurs ordinateurs sur le téléphone lui-même raccordé à la prise Ethernet murale afin de n'utiliser qu'un port réseau (mais deux VLAN), tout port non utilisé de ce commutateur doit être protégé de la même façon.

Authentification des équipements :

- RT 18 : il est RECOMMANDÉ que les équipements de téléphonie s'authentifient en utilisant le protocole 802.1x.

- RT 19 : il est OBLIGATOIRE que les passerelles vers le réseau public commuté (RTC) soient configurées de façon à exiger l'authentification des terminaux qui souhaitent en utiliser les services.

- RT 20 : il est OBLIGATOIRE que les serveurs de téléphonie et les téléphones IP s'authentifient mutuellement, ainsi que les passerelles IP/TDM et les téléphones IP.

- RT 21 : il est RECOMMANDÉ que l'authentification mutuelle entre serveurs de téléphonie et téléphones IP utilise un protocole d'authentification normalisé comme TLS présentant au minimum un certificat du côté du serveur.

- RT 22 : il est OBLIGATOIRE d'identifier et de filtrer les *flux légitimes**. Ces flux peuvent être établis entre les moyens d'extrémité et les serveurs voix ou données, entre le système de ToIP et l'extérieur. Par exemple les flux inter-VLAN sont obligatoirement filtrés (ACL*, listes blanches) au niveau des switches et routeurs. Certaines de ces fonctions peuvent être remplies par une passerelle applicative*, des diodes* ou des ACL.

Authentification des personnes :

- RT 23 : il est OBLIGATOIRE que les connexions aux équipements de téléphonie, nécessaires pour les tâches d'administration et d'exploitation, soient authentifiées (personne) et journalisées, de façon

conforme à la politique de sécurité formalisée.

Interconnexions :

- RT 24 : il est OBLIGATOIRE que les réseaux de téléphonie IP soient interopérables avec la téléphonie commutée ordinaire (TDM*) au moyen de *passerelles homologuées**.

- RT 25 : il est OBLIGATOIRE que l'interconnexion du réseau client de téléphonie avec un opérateur public, pour les appels externes, s'opère au travers d'un tronçon TDM* (rupture de protocole).

- RT 26 : il est INTERDIT de donner accès au réseau de données à travers le service de ToIP (concerne en particulier les messages vocaux et le besoin d'interfaçage d'annuaires de téléphonie et du réseau de données).

- RT 27 : il est DÉCONSEILLÉ de donner accès au réseau de ToIP depuis le réseau de données (concerne en particulier l'usage de téléphones logiciels appelés softphones*, la messagerie vocale et l'interfaçage d'annuaires). Toute demande de dérogation est traitée dans le processus d'homologation.

- RT 28 : pour toute dérogation à la règle précédente, il est OBLIGATOIRE que l'accès aux équipements offrant des services convergés et connectés au réseau de données et au réseau de téléphonie (par exemple : la messagerie unifiée) se fasse via une *passerelle applicative** homologuée, que seule les voies utilisées soient ouvertes et que les connexions soient initiées par le réseau de données et non l'inverse.

- RT 29 : pour toutes les interconnexions autres que celles visées par la règle précédente, il est OBLIGATOIRE que l'interconnexion en IP des différents réseaux internes IP de téléphonie s'opère au travers d'un « Session Border Controler » (SBC*) et d'un système de détection d'intrusion.

Administration, gestion :

- RT 30 : il est OBLIGATOIRE d'activer l'audit, la comptabilité et la journalisation sur les serveurs et passerelles de téléphonie dans le respect de la législation en vigueur. Il est OBLIGATOIRE d'archiver ces journaux conformément à la politique de sécurité formalisée.

- RT 31 : il est OBLIGATOIRE de journaliser les évènements de connexions physiques.

- RT 32 : il est OBLIGATOIRE de garantir le maintien en conditions de sécurité des systèmes composant le système téléphonique (en particulier les systèmes d'exploitation de ces équipements), en appliquant les mesures de protections adéquates définies dans la politique de sécurité formalisée (par exemple gestion des mises à jour, gestion des dispositifs de protections, gestion des incidents).

- RT 33 : il est OBLIGATOIRE si les équipements sont administrés à distance de le faire conformément à la politique de sécurité formalisée.

- RT 34 : il est INTERDIT de stocker les noms d'utilisateurs et les mots de passe dans le terminal d'administration, d'exploitation et de maintenance.

- RT 35 : il est OBLIGATOIRE que les mises à jour logicielles des équipements de téléphonie soient effectuées conformément à la politique de sécurité (contrôle de l'intégrité par signature) et sous le contrôle des administrateurs.

- RT 36 : il est INTERDIT de laisser activés sur les téléphones des services d'accès distant utilisant des protocoles non sécurisés. Ces services doivent être désactivés sur les équipements de téléphonie s'ils sont présents et ne doivent pas pouvoir être réactivés par l'utilisateur.

Sans fil :

- RT 37 : il est DÉCONSEILLÉ d'utiliser les transmissions radios Wi-Fi*.

- RT 38 : il est DÉCONSEILLÉ d'utiliser les transmissions radios DECT*.

- RT 39 : il est DÉCONSEILLÉ d'utiliser les transmissions radios WiMax*.

Protection des flux :

- RT 40 : il est RECOMMANDÉ de protéger les flux de signalisation à l'aide d'un protocole de chiffrement normalisé (tel que par exemple TLS ou SIPS).

Divers :

- RT 41 : il est OBLIGATOIRE d'interdire aux terminaux d'accepter des messages ARP gratuits (GARP).

- RT 42 : il est OBLIGATOIRE d'acheminer localement les appels d'urgence au sens du code des postes et des communications électroniques (numéros : 112, 15, 17, 18, 115 et 119).

- RT 43 : il est OBLIGATOIRE de disposer d'une fonction de téléphonie de secours pour les abonnés ou services vitaux.

- RT 44 : il est OBLIGATOIRE de mettre en œuvre un PCA* incluant un volet ToIP.

- RT 45 : conformément à la PSSI ([PSSI], §4.6.3.3) il est OBLIGATOIRE de mettre en œuvre un PRA* et d'y intégrer le service de ToIP/VoIP au même titre que les autres services du système d'information.

4.1.5. ***Adressage.***

- RT 46 : il est OBLIGATOIRE de se conformer aux règles de gestion des homonymies définies dans la « Charte de nommage Internet » v1.2 du [CCI], règles rappelées en annexe.

- RT 47 : il est OBLIGATOIRE d'affecter des adresses IP aux équipements de téléphonie en conformité avec le plan d'adressage IP du ministère de la défense.

- RT 48 : il est OBLIGATOIRE que tous les équipements de ToIP soient compatibles IP V6.

4.2. **Règles organisationnelles.**

4.2.1. ***Adressage.***

- RO 01 : Il est OBLIGATOIRE que toute personne disposant d'un compte SIP dans un système de téléphonie du ministère de la défense ait un alias de la forme prénomX.nom@nom_de_domaine_Intradef , X correspondant aux caractères supplémentaires permettant de gérer l'homonymie conformément à la charte définie par la règle RT 45.

- RO 02 : si SIP est utilisé, il est OBLIGATOIRE que toute personne n'appartenant pas à un ministère français et travaillant au ministère de la défense dispose d'une adresse SIP de la forme de celle des personnels du ministère de la défense (RO 01) complétée d'un signe distinctif unique : .ext soit une adresse de la forme prénomX.nom.ext@nom_de_domaine_Intradef.

4.2.2. ***Sécurité.***

- RO 03 : En application du décret à paraître du RGS, il est OBLIGATOIRE d'homologuer le système après un processus d'homologation, conforme à l'article 47 de l'IGI 1300, comprenant une étude globale des risques.

- RO 04 : il est RECOMMANDÉ de séparer les rôles et les responsabilités dans l'exploitation du système de téléphonie : celui qui définit la politique de sécurité ne configure pas ; celui qui exploite les traces dans les journaux et la comptabilité ne les configure pas.

- RO 05 : il est OBLIGATOIRE d'exploiter et de consolider les traces de manière continue (comptabilité, journaux applicatifs, relevés d'incidents unitaires). La périodicité des rapports est définie comme une mesure de la politique de sécurité.

- RO 06 : il est OBLIGATOIRE d'effectuer périodiquement et selon les besoins spécifiques des inspections et audits périodiques de l'écart entre la politique de sécurité adéquate choisie formellement, et la situation réelle.

4.3. **Règles sémantiques.**

Sans objet.

Pour le ministre de la défense et par délégation :

Le directeur général des systèmes d'information et de communication,

Henri SERRES.

---

(1) n.i. BO.

ANNEXE I.

GLOSSAIRE ET ACRONYMES.*

802.1ab : 802.1ab est un standard de l'IEEE définissant le protocole LLDP dont le but est de permettre à un agent LLDP, au sein d'un matériel quelconque, de récupérer des informations de connexion et de management auprès de stations (entité compatible IEEE 802) adjacentes.

802.1x : 802.1x est un standard de l'IEEE pour le contrôle d'accès au réseau basé sur les ports. C'est aussi une partie du groupe de protocoles IEEE 802 (802.1). Ce standard fournit une authentification aux équipements connectés à un port Ethernet. Il est aussi utilisé pour certains points d'accès Wi-Fi et est basé sur EAP (RFC 2284, obsolète avec l'arrivée de RFC 3748). 802.1x est une fonctionnalité disponible sur certains commutateurs réseau.

802.3af : standard de l'IEEE définissant le « Power over Ethernet », c'est-à-dire le fait de transférer du courant électrique en même temps que des données. Les câbles restent du RJ45 catégorie 3 ou 5, le courant est en 48V. Étant donné les économies que cela permet et la simplification du câblage, cette norme est promise à un bel avenir. La puissance consommée par l'équipement terminal ne doit pas dépasser 15W.

802.11x : voir Wi-Fi.

ACL (Access Control List) : liste de permissions (lecture, écriture, exécution) sur un fichier, un répertoire ou une arborescence ajoutée aux permissions classiques. Ces permissions concernent des utilisateurs et/ou des groupes définis.

Adresse IP : séquence numérique identifiant un terminal ou un serveur connecté à un réseau IP et permettant à un autre terminal de le contacter.

Dans la version actuelle du protocole IP, l'adresse IP est codée sur 4 octets. Elle est représentée sous forme de 4 nombres décimaux séparés par un point, qui définissent une structure de sous-réseaux hiérarchisés (le dernier nombre représentant le sous-réseau le plus proche de la machine considérée).

Certains blocs d'adresse sont réservés à des usages spéciaux.

Comme de plus en plus d'équipements ont vocation à être reliés à Internet et que le stock d'adresses disponibles menace de s'épuiser, une nouvelle version du protocole, avec un nouveau format d'adresse, IPv6, est en cours d'implémentation.

Adresse MAC (Medium Access Control) : identifiant physique d'une interface réseau, attribuée par l'IEEE et permettant de définir une adresse unique à l'échelon mondial au niveau de la couche liaison (couche 2 du modèle OSI). C'est la partie inférieure de celle-ci (sous-couche d'accès au média - Media access control) qui insère et traite ces adresses au sein des trames transmises.

Appel H.323 : équivalent d'un appel téléphonique entre terminaux H.323. L'adresse du destinataire de l'appel peut être soit son adresse IP, soit son numéro (ou adresse) E.164*.

Antispoofing : lutte contre les usurpations d'identité ou d'adresse.

Authentification : concept ayant pour but de garantir l'identité et les droits associés d'un correspondant dans une transaction à distance. En télécommunication, les procédures correspondantes font généralement appel à des procédés de cryptographie par clé publique ou privée.

Autocommutateur : équipement capable d'établir des connexions temporaires entre des lignes entrantes et sortantes pour acheminer des communications. Commutateur d'abonné (ou commutateur privé) : commutateur téléphonique qui appartient à une installation terminale chez l'abonné et qui est raccordé au réseau général du téléphone. Voir aussi PABX, PBX, IPBX.

Bande passante : différence entre la fréquence la plus haute et la fréquence la plus basse que laisse passer le canal de transmission. Ex. : une ligne téléphonique analogique a une bande passante de 3000 Hz environ ; elle transmet des signaux de 300 à 3400 Hz.

Par extension désigne quelquefois la capacité de transmission d'une ligne numérique, exprimée en bits par seconde.

Bit : contraction des mots anglais « binary digit ». C'est le plus petit élément d'information dans un système binaire. Un bit représente le choix entre l'état qu'il est convenu d'appeler « un » ou « zéro » d'un signal électrique.

Bluetooth : norme de communication sans fil permettant d'établir des petits réseaux personnels, dans un rayon d'une dizaine de mètres (PAN). Ces réseaux s'établissent par exemple entre un kit et une oreillette, un PDA ou un ordinateur.

CDR (Call Detail Record) : enregistrement de données contenant les informations relatives aux appels téléphoniques telles que l'adresse de l'appelant et celle du destinataire, l'heure d'appel et celle de terminaison d'appel, la durée de l'appel et les taxes ajoutées sur le réseau ou la taxation des opérateurs de service.

Chiffrement : moyen par lequel un message est rendu inintelligible en l'absence d'un moyen approprié appelé clef de chiffrement. Les clefs sont basées sur des algorithmes mathématiques.

CNIL : Commission Nationale Informatique et Libertés.

CODEC (Codeur / Décodeur) : élément logiciel ou matériel capable de coder un flux audio ou vidéo et de décoder les flux encodés pour restituer le signal sous une forme analogique. Les divers codecs diffèrent par leurs performances et la qualité des résultats dépend des algorithmes appliqués.

Commutateur : équipement électronique auquel sont raccordés les abonnés et qui permet leur interconnexion.

Commutation : établissement de connexion à la demande et seulement pendant la durée d'une conversation entre des lignes téléphoniques d'abonnés ou, plus généralement, entre des circuits et/ou lignes de transmission.

Commutation de circuits : système dans lequel chaque voie de communication dispose de supports physiques de transmission qui lui sont affectés pendant toute la durée de la communication, même pendant les silences.

Commutation de paquets : technique de télécommunication dans laquelle données et messages à transmettre sont découpés en blocs appelés paquets, contenant un nombre déterminé d'éléments binaires, accompagnés d'informations de service identifiant le paquet et son destinataire. Les différents paquets peuvent emprunter différents chemins.

DCCP (Datagram Congestion Control Protocol) : protocole de la couche transport orienté messages. Les applications qui peuvent bénéficier de DCCP sont celles (Streaming de données, ToIP, etc.) qui ont des contraintes de temps sur la délivrance des données (si les données arrivent trop tard, elles n'ont plus d'utilité) de façon à ce que la délivrance des données soit fiable et ordonnée dès lors qu'un système de gestion des congestions est utilisé. La gestion des congestions est le moyen pour un protocole réseau de découvrir la capacité disponible sur un chemin donné.

DECT (Digital Enhanced Cordless Telephone) : norme de téléphonie sans fil, fonctionnant dans la bande des 1800 MHz, définie à la fin des années 80 par l'ETSI. Le DECT permet d'offrir des services de téléphonie de proximité autour d'un autocommutateur d'entreprise ou d'un poste résidentiel. Les postes portatifs peuvent dialoguer entre eux et prendre une liaison externe.

DHCP (Dynamic Host Configuration Protocol) : protocole permettant d'attribuer une adresse IP temporaire aux machines souhaitant se connecter à un réseau IP.

DiffServ (Differential Service) : alternative au protocole RSVP, jugé trop complexe pour des réseaux étendus. Ce type de service vise à utiliser les champs de QoS d'ores et déjà disponibles avec IPv4 et IPv6. Face à la demande croissante de transmission de flux multimédia, les équipements du réseau intègrent aujourd'hui les algorithmes permettant le traitement du champ TOS d'IP. Le principe de DiffServ est d'accorder un traitement particulier au paquet le nécessitant. Il s'agit en fait d'un aménagement du « best effort » IP sans fournir strictement de la QoS.

Diode : dispositif permettant d'interconnecter deux réseaux de niveau de sécurité différents, fournissant un canal de communication ne fonctionnant que dans un sens. Cela permet d'empêcher que des informations du réseau de sécurité haute soient transmises au réseau de niveau de sécurité inférieure.

DNS (Domain Name System) : protocole permettant de convertir les noms de domaines alphabétiques connus des utilisateurs d'Internet (par exemple : afutt.org) en adresses IP reconnues par les routeurs qui acheminent les paquets à travers le réseau. L'ensemble des serveurs DNS forme un réseau au sein du réseau Internet, chaque serveur pouvant interroger d'autres serveurs lorsqu'il ne trouve pas la correspondance « Nom de domaine/Adresse IP » dans sa base de données.

DTMF (Dual tone multi-frequency - en français : Signalisation multifréquences) : une des signalisations utilisées en téléphonie. Elle consiste à combiner deux fréquences prises parmi cinq (700, 900, 1100, 1300 et 1500 Hz). Cette signalisation est utilisée notamment lorsque l'on effectue la numérotation de son correspondant.

E.164 : recommandation de l'UIT, actuellement utilisée pour la numérotation téléphonique au plan mondial.

ENUM (Electronic Number) : standard pour la conversion des numéros E.164 en adresse Internet et réciproquement aux fins de téléphonie sur IP (RFC 2916).

Equipement légitime : équipement autorisé par la politique de sécurité.

Facilités téléphoniques : ensemble de fonctionnalités, permettant d'enrichir la fonction de base de téléphonie, telles que le transfert d'appel, le filtrage patron - secrétaire, la mise en attente, etc.

Firewall : voir pare-feu.

Flux légitime : flux entre deux équipements conforme à la politique de sécurité.

Gatekeeper (GK) : élément logiciel fonctionnant dans un PC ou dans un pont multipoint* capable de router un appel H.323 dans le réseau, en fonction de l'adresse de destinataire contenue dans l'appel. Il gère les appels H.323 qui arrivent au pont multipoint* et les envoie vers la bonne conférence parmi celles actives dans le MCU*.

Gigue : Variation anormale de la périodicité lors de la transmission d'un signal, notamment lorsqu'il est multiplexé.

H.323 : protocole défini par l'UIT-T pour permettre la téléphonie sur Internet.

Interopérabilité : aptitude qu'ont des équipements terminaux à fonctionner d'une part avec le réseau et d'autre part avec les autres équipements terminaux permettant d'accéder à un même service.

IP (Internet Protocol) : protocole d'interconnexion de réseaux et/ou machines hétérogènes pour la transmission de données par paquets sur Internet.

Isochrone : se dit de données quand les éléments d'information qui les composent sont liés par une récurrence temporelle stricte.

Exemple : pour reconstituer parfaitement la voix, il est nécessaire que tous les échantillons soient reçus à la même cadence que celle de l'échantillonnage (125 ms pour la numérisation G.711).

Les systèmes de transmission de données sur IP étant incapables de respecter cette contrainte (gigue du réseau), les systèmes de réception sont dotés d'un buffer élastique délivrant les données à la bonne cadence (buffer correcteur de gigue : temps moyen de rétention d'environ 50 ms à prendre en compte dans le bilan temporel global du système).

ITU (International Telecommunication Union) : voir UIT.

comment on accède et met à jour l'information, un modèle de distribution permettant de répartir les données (à partir de la v3), un protocole et un modèle de données extensible, des API pour développer des applications clientes.

LDAP (Lightweight Directory Access Protocol) : protocole normalisé par l'IETF, définissant une méthode d'accès à un annuaire.

Messagerie électronique (courrier électronique, e-mail, courriel) : service permettant d'échanger des messages écrits et de les stocker dans des boîtes aux lettres électroniques relevées à l'initiative du destinataire. Ceci évite aux correspondants d'être connectés au réseau simultanément. Il est possible d'attacher aux messages des fichiers de type texte, son, image, vidéo. Ce service autorise le multi-adressage.

Messagerie instantanée : mécanisme de discussion « en temps réel » (diffère de la messagerie électronique qui a été conçue pour un usage désynchronisé) entre les membres d'une liste de correspondants favoris Ceux-ci sont informés lorsque l'un d'eux se connecte à Internet ce qui leur permet d'entamer une conversation.

Messagerie unifiée : système de messagerie regroupant les messages électroniques, les messages vocaux voire les télécopies destinés à un même destinataire.

Messagerie vocale : système d'enregistrement, de stockage, d'écoute, voire de ré-expédition, de messages vocaux, fonctionnant comme un répondeur téléphonique partagé par plusieurs utilisateurs.

MGCP (Media Gateway Control Protocol) : protocole asymétrique (client-serveur) de VoIP, par opposition à SIP et H323 qui sont symétriques (client-client). Les FAI par ADSL français utilisent en règle générale ce protocole pour la téléphonie. MGCP est à la base des services de téléphonie de type Centrex.

NAT (Network Address Translation - RFC 1631 et RFC 1519) : moyen permettant à des machines sur des réseaux différents, utilisant des plans d'adressage incompatibles, de communiquer de façon transparente.

NTP (Network Time Protocol) : protocole permettant de synchroniser les horloges des systèmes informatiques à travers un réseau de paquets, dont la latence est variable.

Pare-feu : solution de sécurisation des accès informatiques d'une entreprise. En technologie Internet, le pare-feu est interposé entre le réseau interne de l'entreprise et les accès aux réseaux extérieurs. Le pare-feu fonctionne comme un sas de décontamination des paquets IP et des services indésirables.

Passerelle : équipement et/ou logiciel assurant l'inter-fonctionnement entre des réseaux utilisant des protocoles de communication différents.

Passerelle applicative : pare-feu* effectuant du filtrage au niveau applicatif (couche 7 du modèle OSI). Contrairement au filtrage de paquets simple (niveau 4), le filtrage applicatif présuppose une connaissance des protocoles utilisés par les applications.

Passerelle homologuée : passerelle ayant fait l'objet d'une homologation au sens de l'IGI 1300.

PCA (Plan de Continuité d'Activité) : ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée de l'activité. C'est donc un mode planifié et formalisé de réaction à un sinistre en vue de diminuer ses impacts adverses sur l'activité de l'entreprise. C'est plus qu'un plan de secours informatique, plus qu'un plan de gestion de crise, plus qu'un plan de reprise d'activité, plus qu'un plan de continuité opérationnel, plus que des procédures de fonctionnement dégradé : on pourrait dire que c'est tout cela, coordonné.

Port : terme anglais désignant l'interface (physique ou logicielle) d'une ligne ou d'un équipement.

PRA (Plan de Reprise d'Activité) : plan permettant de répondre au besoin du redémarrage rapide de l'activité suite à un sinistre occasionnant la perte partielle ou totale du site informatique de production. Il se traduit par :

- une infrastructure matérielle/logicielle et des procédures de transfert de données assurant une copie sécurisée des applications et données vitales pour l'entreprise ;

- des procédures d'accès au système ainsi que les processus humains permettant le redémarrage des services.

Protocole : ensemble de spécifications qui permettent à deux matériels ou logiciels en réseau de communiquer. Ils s'appliquent à diverses opérations, dont l'établissement des connexions, le codage et le contrôle des erreurs.

Q.931 : protocole de signalisation utilisé en VoIP pour les communications RNIS. Q.931 initie et termine les appels.

QoS (Quality of Service - En français : qualité de service) : recouvre des ensembles de plus en plus souvent formalisés de critères permettant d'évaluer le service rendu.

Les critères varient selon le type de service, mais on retrouve souvent, au-delà de la qualité des réseaux (débit annoncé...), des critères liés à l'accueil client, au service après-vente, à la disponibilité, à la réactivité, avec des engagements contractualisés. Voir aussi SLA.

QSIG : protocole de signalisation compatible avec le système de signalisation par canal sémaphore n° 7 (SS7) permettant l'interconnexion de PABX hétérogènes.

RFC : Request For Comment : série de documents et normes concernant l'Internet. Peu de RFC sont des standards mais tous les standards de l'Internet sont enregistrés en tant que RFC.

Réseau maîtrisé : réseau sur lequel on peut faire appliquer une PSSI, des mesures de détection et de rétorsion.

Routage : opération effectuée par un routeur situé sur un nœud de communication. Le routage permet d'analyser dynamiquement les adresses de destination des paquets incidents et de les orienter, à partir de tables de routage évolutives, sur le meilleur chemin possible en fonction de leur priorité et de la nature de trafic à transporter, ainsi que de la qualité et de la disponibilité offertes par le réseau à un instant donné.

RSVP (Resource Reservation Protocol) : protocole de gestion réseau qui permet aux applications d'obtenir des qualités de service différentes (QoS). Une telle capacité repose sur le fait que des applications différentes n'ont pas les mêmes exigences de performance du réseau. RSVP n'est pas un protocole de routage* mais travaille avec de tels protocoles. Il installe l'équivalent de listes d'accès dynamiques le long des routes élaborées par les protocoles de routage.

RTC (Réseau Téléphonique Commuté - En anglais : PSTN ou Public Switched Telecommunication Network) : réseau permettant l'établissement de communications point à point par commutation de circuits. Ce réseau offre un débit numérique ou une bande passante garantie qui peut être utilisée pour transmettre des données informatiques, des télécopies, etc. par utilisation d'un modem.

RTCP (Real-time Transport Control Protocol) : protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session et sur la qualité de service. Il s'appuie sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session.

RTP (Real-time Transport Protocol) : protocole de transmission de données IP ayant des contraintes de temps réel (audio, vidéo...). Le rôle principal de RTP consiste à mettre en œuvre des numéros de séquence de paquets IP pour reconstituer les informations de voix ou vidéo même si le réseau sous-jacent change l'ordre des paquets.

RTSP (Real Time Streaming Protocol) : protocole développé par l'IETF (RFC 2326) et utilisé par les systèmes de streaming média pour permettre à un client de contrôler le serveur média à l'aide de commandes similaires aux commandes de magnétoscope telles que « lecture », « pause » et permettant un accès basé sur le temps aux fichiers sur un serveur. La plupart des serveurs RTSP utilisent le protocole RTP pour transporter les données audio et vidéo.

SBC (Session Border Controller) : équipement placé en bordure de réseau et destiné à contrôler les flux de signalisation et media de la VoIP*. Il comprend habituellement les composants suivants :

- analyse protocolaire de la signalisation ;
- contrôle d'accès et management de la bande passante ;
- ouverture des ports nécessaires aux communications sur le pare-feu ;
- traversée de pare-feu avec translation d'adresse de « NAT*/STUN* » (NAT/Firewall traversal) ;
- contrôle d'émission des appels ;
- transport de la signalisation entre réseaux (réécriture d'un réseau à l'autre) ;
- normalisation de la facturation et des CDRs* ;
- Analyse protocolaire des flux media (DTMF*, CODEC*) ;
- sécurisation de la signalisation ;
- protection contre le déni de service (DOS*) ;
- dissimulation de la topologie ;
- conversion de « CODEC* » média.

SCTP (Stream Control Transmission Protocol) : protocole défini en 2000 par l'IETF (RFC 2960). En tant que protocole de transport, SCTP est équivalent dans un certain sens à TCP ou à UDP. En effet, il fournit des services similaires à TCP, assurant la fiabilité, la remise en ordre des séquences, et le contrôle de congestion. Alors que TCP est « orienté octets », SCTP gère des « frames » (courtes séquences). Une avancée majeure de SCTP est la possibilité de communications multi-cibles, où une des extrémités (voire toutes) de la connexion est constituée de plusieurs adresses IP.

SFTP : protocole de communication fonctionnnant au dessus de SSH pour transférer et gérer des fichiers à distance.

Signalisation téléphonique : ensemble des ordres ou informations échangés entre autocommutateurs ou entre un autocommutateur et un poste, afin d'établir, maintenir ou terminer une communication.

- Signalisation téléphonique par canal sémaphore (SS7) :

Technique de signalisation dans laquelle les informations de signalisation relatives à un circuit ne sont pas transmises sur ce circuit mais sur des canaux sémaphores indépendants ne transmettant que des données. Le système le plus répandu est le code CCITT n° 7.

- Signalisation téléphonique RON-TRON :

Méthode de signalisation, hors bande ou dans la bande par laquelle l'information de signalisation est restituée aux extrémités sur les équipements de commutation et de transmission au moyen de fils conducteurs spécialisés, appelés RON (Réception par l'autocommutateur) et TRON (Transmission par l'autocommutateur).

SIP : (Session Initiation Protocol). Protocole de niveau application basé sur TCP/IP pour l'établissement de sessions d'appels en téléphonie sur IP. Ce protocole défini par l'IETF est concurrent du protocole H323.

SNMP (Simple Network Management Protocol) : protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et des matériels à distance.

Softphone : logiciel émulant sur un équipement informatique la fonction de terminal de téléphonie est appelé softphone par analogie au software pour le logiciel et par opposition au « hard ».

SSH : programme informatique et protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Ensuite, toutes les trames sont chiffrées. Le protocole SSH a été conçu pour remplacer les programmes rlogin, telnet et rsh.

TDM : (Time Division Multiplexing) : méthode de multiplexage des signaux électriques numériques, issus du codage de la voix et obtenus par échantillonnage, permettant de les acheminer dans une trame de 30 intervalles de temps, pour être ensuite correctement aiguillés par les matrices de commutation des autocommutateurs traditionnels du réseau téléphonique commuté (RTC). L'appellation « réseau TDM » est souvent utilisée par les professionnels de la téléphonie pour distinguer les réseaux téléphoniques commutés (RTC), des réseaux fonctionnant sous le protocole Internet (IP) qui sont basés sur la transmission de paquets aiguillés par des routeurs.

Téléphonie : application temps réel qui « travaille » avec des flux isochrones. La diffusion vidéo ou sonore n'est pas temps réel, seuls les flux sont qualifiés d'isochrone.

Téléphonie administrative : téléphonie standard par opposition à la téléphonie opérationnelle.

Temps réel : propriété des applications dont les données manipulées ont une durée de validité prédéterminée. Ce sont des applications dites aussi à temps borné.

Exemple : la transmission de l'heure avec une précision d'une seconde demande à ce que le temps de réponse du système soit inférieur à la seconde, sinon l'information reçue est erronée.

Dans le cas d'une application interactive, la notion de temps réel recouvre celle du fonctionnement correct de l'application. Pour assurer une communication téléphonique correcte, le temps de bouche à oreille (appelé aussi temps *bo*) doit être inférieur à 150 ms (ITU-T G.114).

Terminal : équipement situé au domicile d'un client ou affecté à un poste de travail dans une entreprise et qui permet à son utilisateur d'accéder à un réseau de télécommunications. Voir aussi Équipement terminal.

TFTP (Trivial File Transfer Protocol) : protocole simplifié de transfert de fichiers qui ne gère pas l'affichage de liste des fichiers ni l'authentification ni le chiffrement. C'est un protocole très utilisé pour effectuer les mises à jour des logiciels embarqués dans les équipements réseaux.

TLS (Transport Layer Security) : norme de sécurisation du transport de l'information. Elle offre des mécanismes d'authentification du serveur, du client en option, ainsi que des mécanismes d'intégrité et de confidentialité du transport. Nécessite l'utilisation de certificats électroniques d'authentification de type X509V3.

ToIP : (Telephone over IP - Téléphonie sur IP) : service de téléphonie par IP qui utilise le protocole IP pour le transport de la voix et l'établissement des communications au niveau de l'accès ou du coeur du réseau.

VLAN : réseau virtuel créé au sein d'un LAN, totalement séparé du reste du LAN. Un équipement situé sur un VLAN ne peut entrer en relation avec un équipement situé sur un autre VLAN que si un routeur lui en donne l'autorisation. Le VLAN répond donc souvent à un besoin de sécurité.

VoIP : (Voice over IP - Voix sur IP) : transmission de la voix téléphonique en mode paquet sur un réseau qui utilise le protocole IP.

Wi-Fi (contraction de Wireless Fidelity) : marque commerciale déposée, définissant un système de transmission de données par radio de type R-LAN dans la norme 802.11 et complétée par un système de chiffrement des données pour assurer un premier niveau de sécurité. Désigne couramment le réseau radio utilisant ce système et permettant un accès sans fil à Internet.

WiMax (Worldwide Interoperability for Microwave Access) : technique de boucle locale radio pour la transmission de données à haut débit définie par la norme IEEE 802.16. En 2005, l'objectif des opérateurs WiMax est de pouvoir proposer à moyen terme un débit de 10Mb/s sur une distance de 8 Km.

XMPP (eXtensible Messaging and Presence Protocol) : protocole s'appuyant sur XML et développé par Jeremie Miller en 1998 pour le système de messagerie instantanée Jabber et comprenant la messagerie instantanée, la présence, la syndication de contenu ainsi que des fonctions collaboratives telles que le tableau blanc.

ANNEXE II.
RÉFÉRENCES.

[Loi1991] - loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques

[IGI 1300] - Instruction générale interministérielle sur la protection du secret de la Défense nationale n° 1300 SGDN/PSE/SSD (1) du 25 août 2003.

[IGI 901] - Recommandation 901/DISSI/SCSSI du 2 mars 1994.

[CCI] - Recommandations nationales du cadre commun d'interopérabilité des systèmes d'information publics. Circulaires du Premier Ministre du 21 janvier 2002 et du 4 décembre 2002.

[RGI] - Référentiel Général d'Interopérabilité

[RGS] - Référentiel Général de Sécurité

[PRIS] Politique de Référencement Intersectoriel de Sécurité v2.0 du 1er juin 2005 (ADAE et DCSSI).

[OSCAR] - Directive d'orientation pour la sécurisation des interconnexions et des architectures de réseaux « OSCAR » diffusée par la note n° 178/DEF/SEC.DIR.SIC du 4 mai 2001 (1).

[PSSI] - Instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'information du ministère de la défense .

[DGSIC001] - Directive n° 1/DEF/DGSIC du 17 octobre 2006 portant sur les logiciels du ministère de la défense

[DGSIC002] - Directive n° 2/DEF/DGSIC du 9 mars 2007, modifiée portant sur le système d'annuaires (SA) du ministère de la défense

[DGSIC003] - Directive n° 3/DEF/DGSIC du 8 janvier 2008 définissant les règles de la messagerie électronique

[OSCAR] - Directive d'orientation pour la sécurisation des interconnexions et des architectures de réseaux « OSCAR » diffusée par la note n° 178/DEF/SEC.DIR.SIC du 4 mai 2001 (1).

[IM8192] - Instruction n° 8192/DEF/SEC.DIR.SIC du 30 juin 2003 relative aux modalités d'accès, de raccordement et d'utilisation des réseaux externes au ministère de la défense.

[EMA1233] - Note n° 1233/DEF/EMA/PI/-- du 2 juin 2005 (1) (version 2.1) relative à la politique d'interconnexion des réseaux IP de la défense.

[PSI1] - Politique de sécurité de l'Intradef version 1.0 du 4 décembre 2000 diffusée par la note n° 2448/DEF/EMA/TSIC/4 du 6 décembre 2000 (1).

[DIRSIC365] - Note n° 365/DEF/SEC/DIR/SIC du 25 juillet 2002 (1) relative aux dangers de l'utilisation des réseaux sans fil.

[DGSIC259] - Note n° 259/DEF/DGSIC du 15 juin 2006 (1) relative aux spécifications de sécurisation et régime dérogatoire pour les nouvelles technologies.

[CNIL] - Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

[CPCE] - Code des postes et des communications électroniques.

[CMTSIC1] - Compte rendu de la 4e CMTSIC n° 262/DEF/DGSIC/SDAI du 10 mai 2007 (1).

[GTEP] : Groupe de Travail spécialisé dans l'Examen des projets SIAG et SIOC. Les modalités de présentation des projets de SIAG au GTEP de la CSIAG sont fixées par l'instruction n° 713/DEF/SGA du 24 juin 2004 (1).

Recommandations CELAR.

Note n° 2006-101330/CELAR/TEC/RX/1703328/NC du 21 avril 2006 Version 1.0.

Security Guidance for Deploying IP Telephony Systems

SNAC (NSA) - version 1.01 - 14 février 2006 - (US)

Recommended IP Telephony Architecture

SNAC (NSA) - version 1.0 - 1er mai 2006 - (US)

Internet Protocol Telephony and Voice Over Internet Protocol Security Technical Implementation Guide Developed by DISA for the DoD - Version 2, Release 1 - 21 avril 2006 - (US)

Les RFC sont consultables à l'adresse suivante : http://www.ietf.org/rfc/rfcnumero de RFC.txt

[RFC 2326] - Real Time Streaming Protocol (RTSP) (Proposed Standard 04/1998)

[RFC 2352] - Extended facsimile using internet mail (Proposed Standard 03/1999)

[RFC 2805] - Media Gateway Control Protocol Architecture and Requirements (Informational 04/2000)

[RFC 3261] - SIP : Session Initiation Protocol (mis à jour par RFC 4916) (Proposed Standard 06/2002)

[RFC 3262] - Reliability of provisional responses in Session Initiation Protocol (SIP) (Proposed Standard 06/2002)

[RFC 3263] - Session Initiation Protocol (SIP) locating SIP servers (Proposed Standard 06/2002)

[RFC 3264] - An offer/answer model with Session Description Protocol (SDP) (Proposed Standard 06/2002)

[RFC 3265] - Session Initiation Protocol (SIP) - specific event notification (met à jour le RFC 3261) (mis à jour par RFC 5367) (Proposed Standard 06/2002)

[RFC 3312] - Integration of resource management and Session Initiation Protocol (SIP) (Proposed Standard 11/2002)

[RFC 3319] - Dynamic Host Configuration Protocol (DHCPv6) options for Session Initiation Protocol (SIP) servers (Proposed Standard 07/2003)

[RFC 3327] - Session Initiation Protocol (SIP) extension header field for registering non-adjacent contacts (Proposed Standard 12/2002)

[RFC 3329] - Security mechanism agreement for the Session Initiation Protocol (SIP) (Proposed Standard 01/2003)

[RFC 3331] - Signalling System 7 (SS7) Message Transfer Part 2 (MTP2) - User adaptation layer (Proposed Standard 09/2002)

[RFC 3362] - Real-time facsimile (T.38) - image/t38 MIME Sub-type registration (Proposed Standard 08/2002)

[RFC 3398] - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping (Proposed Standard 12/2002)

[RFC 3428] - Session Initiation Protocol (SIP) extension (Proposed Standard 12/2002)

[RFC 3435] - Media Gateway Control Protocol (MGCP) version 1.0 (Informational 01/2003)

[RFC 3436] - Transport Layer Security over Stream Control Transmission Protocol (Proposed Standard 12/2002)

[RFC 3487] - Requirements for resource priority mechanisms for the Session Initiation Protocol (SIP) (Informational 02/2003)

[RFC 3525] - Megaco Protocol version 1 (Proposed Standard 06/2003)

[RFC 3550] - RTP : a Transport Protocol for Real-Time applications (Standard 07/2003)

[RFC 3551] - RTP Profile for audio and video conferences with minimal control (Standard 07/2003)

[RFC 3554] - On the use of Stream Control transmission Protocol (SCTP) with IPsec (Proposed Standard 07/2003)

[RFC 3556] - session description Protocol (SDP) bandwidth modifiers for RTP Control Protocol (RTCP) bandwidth (Proposed Standard 07/2003)

[RFC 3578] - Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) overlap signalling to the Session Initiation Protocol (SIP) (Proposed Standard 08/2003)

[RFC 3581] - An extension for the Session Initiation Protocol (SIP) for symmetric response routing (Proposed Standard 08/2003)

[RFC 3605] - Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) (Proposed Standard 10/2003)

[RFC 3611] - RTP control protocol extended reports (RTCP XR) (Proposed Standard 11/2003)

[RFC 3640] - Payload format for transport of MPEG-4 elementary streams (Proposed Standard 11/2003)

[RFC 3660] - Basic Media Gateway Control Protocol (MGCP) Packages (Informational 12/2003)

[RFC 3661] - Media Gateway Control Protocol (MGCP) return code usage (met à jour RFC 3435) (Informational 12/2003)

[RFC 3666] - Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) call flows (Best Current Practice 12/2003)

[RFC 3711] - The Secure Real-Time Transport Protocol (SRTP) (Proposed Standard 03/2004)

[RFC 3758] - Stream control Transmission Protocol (SCTP) partial reliability extension (Proposed Standard 05/2004)

[RFC 3761] - The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) application (ENUM) (Proposed Standard 04/2004)

[RFC 3762] - Telephone Number Mapping (ENUM) service registration for H.323 (Proposed Standard 04/2004)

[RFC 3807] - V5.2 user adaptation layer (V5UA) (Proposed Standard 06/2004)

[RFC 3853] - S/MIME Advanced Encryption Standard (AES) requirement for the Session Initiation Protocol (SIP) (Proposed Standard 07/2004)

[RFC 3856] - A presence event package for the Session Initiation Protocol (SIP) (Proposed Standard 08/2004)

[RFC 3868] - Signalling Connection Control part user adaptation layer (SUA) (Proposed Standard 10/2004)

[RFC 3873] - Stream Control transmission Protocol (SCTP) Management Information Base (MIB) (Proposed Standard 09/2004)

[RFC 3893] - Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) format (Proposed Standard 09/2004)

[RFC 3951] - Internet Low Bit Rate (iLBC) (Experimental 12/2004)

[RFC 3953] - Telephone Number Mapping (ENUM) service registration for presence services (Proposed Standard 01/2005)

[RFC 3959] - The early session disposition type for the Session Initiation Protocol (SIP) (Proposed Standard 12/2004)

[RFC 3960] - Early media and ringing tone generation in the Session Initiation Protocol (SIP) (Informational 12/2004)

[RFC 4032] - Update to the Session Initiation Protocol (SIP) preconditions framework (Proposed Standard 03/2005)

[RFC 4142] - Full-mode Fax Profile for Internet Mail (FFPIM) (Proposed Standard 11/2005)

[RFC 4143] - Facsimile Using Internet Mail (IFAX) service of ENUM (Proposed Standard 11/2005)

[RFC 4168] - The Stream Control transmission Protocol (SCTP) as a transport for the Session Initiation Protocol (SIP) (Proposed Standard 10/2005)

[RFC 4233] - Integrated Services Digital Network (ISDN) Q.921 - user adaptation layer (mis à jour par RFC 5133) (Proposed Standard 01/2006)

[RFC 4320] - Actions addressing identified issues with the Session Initiation Protocol's (SIP) non-INVITE transaction (met à jour le RFC 3261) (Proposed Standard 01/2006)

[RFC 4411] - Extending the Session Initiation Protocol (SIP) reason header for pre-emption events (Proposed Standard 02/2006)

[RFC 4414] - An ENUM registry type for the Internet Registry Information Service (IRIS) (Proposed Standard 02/2006)

[RFC 4458] - Session Initiation Protocol (SIP) URIs for applications such as Voicemail and Interactive Voice Response (IVR) (Informational 04/2006)

[RFC 4474] - Enhancements for authenticated identity management in the Session Initiation Protocol (SIP) (Proposed Standard 08/2006)

[RFC 4479] - A Data model for presence (Proposed Standard 07/2006)

[RFC 4497] - Internetworking between the Session Initiation Protocol (SIP) and QSIG (Best Current Practice 11/2006)

[RFC 4567] - Key management extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP) (Proposed Standard 07/2006)

[RFC 4571] - Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) packets over connection-oriented transport (Proposed Standard 07/2006)

[RFC 4572] - Connection-oriented media transport over the Transport Layer Security (TLS) protocol in the Session Description Protocol (SDP) (Proposed Standard 06/2006)

[RFC 4585] - Extended RTP profile for Real-time Transport Control Protocol (RTCP)-based feedback (RTP/AVPF) (Proposed Standard 07/2006)

[RFC 4588] - RTP retransmission payload format (Proposed Standard 07/2006)

[RFC 4666] - Signalling System 7 (SS7) Message Transfer Part 3 (MTP3) - user adaptation layer (M3UA) (Proposed Standard 09/2006)

[RFC 4733] - RTP Payload for DTMF digits, telephony tones and telephony signals (mis à jour par RFC 4734) (mis à jour par RFC 5244) (Proposed Standard 12/2006)

[RFC 4734] - Definition of events for modem, fax and text telephony signals (met à jour RFC 4733) (Proposed Standard 12/2006)

[RFC 4740] - Diameter Session Initiation Protocol (SIP) application (Proposed Standard 11/2006)

[RFC 4759] - The ENUM Dip indicator parameter for the tel URI (Proposed Standard 12/2006)

[RFC 4769] - IANA Registration for an Enum service containing Public Switched Telephone Network (PSTN) (Proposed Standard 11/2006)

[RFC 4780] - Management Information Base for the Session Initiation Protocol (SIP) (Proposed Standard 04/2007)

[RFC 4820] - Padding chunk and parameter for the Stream Control transmission Protocol (SCTP) (Proposed Standard 03/2007)

[RFC 4825] - The Extensible Markup Language (XML) Configuration Access Protocol (XCAP) (Proposed Standard 05/2007)

[RFC 4826] - Extensible Markup Language (XML) formats for representing resource lists (Proposed Standard 05/2007)

[RFC 4827] - An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) usage for manipulating presence document contents (Proposed Standard 05/2007)

[RFC 4916] - Connected Identity in the session Initiation Protocol (SIP) (Proposed Standard 06/2007)

[RFC 4960] - Stream Control Transmission Protocol (Proposed Standard 09/2007)

[RFC 5133] - Terminal Endpoint Identifier (TEI) Query Request Number Change (Proposed Standard 12/2007)

[RFC 5244] - Definition of Events for Channel-Oriented Telephony Signalling (Proposed Standard 06/2008)

[RFC 5367] - Subscriptions to Request-Contained resource Lists in the Session Initiation Protocol (SIP) (Proposed Standard 10/2007)

Les Recommandations de l'UIT sont tenues à jour sur leur site : http://www.itu.int/

[G.165] Echo cancellers (03/1993)

[G.168] - Digital network echo cancellers (08/2004)

[G.711] - Pulse Code Manipulation (PCM) of voice frequencies (11/1988)

[G.722] - 7 KHz audio-coding within 64 kbit/s (11/1988)

[G.723.1] - Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s (05/2006)

[G.726] - 40, 32, 24, 16 kbit/s Adaptative Differential Pulse Code Modulation (ADPCM) (12/1990)

[G.727] - 5-, 4-, 3- and 2- bit/sample embedded adaptive differential pulse code modulation (ADPCM) (12/1990)

[G.728] - Coding of speech at 16kbit/s using low-delay code excited linear prediction (09/1992)

[G.729] - Coding of speech at 8 kbit/s using conjugate-structure algebraic code-excited linear prediction (CS-ACELP) (03/1996)

[H.225.0] - Call signalling protocols and media stream packetization for packet-based multimedia communication systems H.235.1 (05/2006)

[H.235.0] - H.323 Security : Framework for security in H series (H.323 and other H.245 based) multimedia systems (09/2005)

[H.235.1] - H.323 Security : Basic security profile (09/2005)

[H.235.2] - H.323 Security : Signature security profile (09/2005)

[H.235.3] - H.323 Security : Hybrid security profile (09/2005)

[H.235.4] - H.323 Security : Direct and selective routed call security (09/2005)

[H.235.5] - H.323 Security : Framework for secure authentication in RAS using weak shared secrets (09/2005)

[H.235.6] - H.323 Security : Voice encryption profile with native H.235/H.245 key management (09/2005)

[H.235.7] - H.323 Security : Usage of MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235 (09/2005)

[H.235.8] - H.323 Security : Security gateway support for H.323 (09/2005)

[H 245] - Control protocol for multimedia communication (05/2006)

[H.248.1] - Gateway control protocol : Version 3 (09/2005)

[H.248.2] - Gateway control protocol : Facsimile, text conversation and call discrimination packages (01/2005)

[H.248.3] - Gateway control protocol : User interface elements and actions packages (11/2000)

[H.248.4] - Gateway control protocol : Transport over Stream Control Transmission Protocol (SCTP) (11/2000)

[H.248.5] - Gateway control protocol : Transport over ATM (11/2000)

[H.248.6] - Gateway control protocol : Dynamic tone definition package (11/2000)

[H.248.7] - Gateway control protocol : Generic Announcement package (03/2004)

[H.248.8] - Gateway control protocol : Error code and service change reason description (09/2005)

[H.248.9] - Gateway control protocol : Advanced media server package (01/2005)

[H.248.10] - Gateway control protocol : Media gateway resource congestion handling package (07/2001)

[H.248.11] - Gateway control protocol : Media gateway overload control package (11/2002)

[H.248.12] - Gateway control protocol : H.248.1 packages for H.323 and H.324 internetworking (07/2001)

[H.248.13] - Gateway control protocol : Quality Alert Ceasing package (03/2002)

[H.248.14] - Gateway control protocol : Inactivity timer package (03/2002)

[H.248.15] - Gateway control protocol : SDP H.248 package attribute (03/2002)

[H.248.16] -Gateway control protocol : Enhanced digit collection packages and procedures (11/2002)

[H.248.17] - Gateway control protocol : Line test packages (11/2002)

[H.248.18] - Gateway control protocol : Package for support of multiple profile (11/2002)

[H.248.19] - Gateway control protocol : Decomposed multipoint control unit, audio, video and data conferencing packages (03/2004)

[H.248.20] - Gateway control protocol : The use of local and remote descriptors with H.221 and H.223 multiplexing (11/2002)

[H.248.21] - Gateway control protocol : Semi-permanent connection handling package (03/2004)

[H.248.22] - Gateway control protocol : Shared Risk Group package (07/2003)

[H.248.23] - Gateway control protocol : Enhanced Alerting packages (01/2005)

[H.248.24] - Gateway control protocol : Multi-frequency tone generation and detection packages (07/2003)

[H.248.25] - Gateway control protocol : Basic CAS packages (01/2007)

[H.248.26] - Gateway control protocol : Enhanced analog lines package (01/2005)

[H.248.27] - Gateway control protocol : Supplemental tones package (07/2003)

[H.248.28] - Gateway control protocol: International CAS package (03/2004)

[H.248.29] - Gateway control protocol : International CAS compelled register signaling packages (01/2005)

[H.248.30] - Gateway control protocol : RTCP extended performance metrics packages (01/2007)

[H.248.31] - Gateway control protocol : Adaptive jitter buffer package (04/2004)

[H.248.32] - Gateway control protocol : Detailed congestion reporting package (01/2005)

[H.248.33] - Gateway control protocol : PCM frame spare bit packer (01/2005)

[H.248.34] - Gateway control protocol : Stimulus analogue lines package (01/2005)

[H.248.35] - Gateway control protocol : Coin package (01/2005)

[H.248.36] - Gateway control protocol : Hanging Termination Detection package (09/2005)

[H.248.37] - Gateway control protocol : IP NAPT traversal package (09/2005)

[H.248.38] - Gateway control protocol : Base context package (05/2006)

[H.248.39] - Gateway control protocol : H.248 SDP parameter identification and wildcarding (05/2006)

[H.248.40] - Gateway control protocol : Application Data Inactivity Detection Package (01/2007)

[H.248.41] - Gateway control protocol : IP domain connection package (05/2006)

[H.248.42] - Gateway control protocol : DCME internetworking package (05/2006)

[H.248.44] - Gateway control protocol : Multi-level precedence and pre-emption package (01/2007)

[H.248.45] - Gateway control protocol : MGC information package (05/2006)

[H.248.46] - Gateway control protocol : Connection Capability Control package (01/2007)

[H.248.47] - Gateway control protocol : Statistic conditional reporting package (01/2007)

[H.261] - Video codec for audiovisual services at p x 64 kbit/s (03/1993)

[H.262] - Information technology - Generic coding of moving pictures and associated information: Video (02/2000)

[H.263] - Video coding for low bit rate communication (01/2005)

[H.264] - Advanced video codec for generic audiovisual services (03/2005)

[H.264.1] - Conformance specification for H.264 advanced video coding (03/2005)

[H.264.2] - Reference software for H.264 advanced video coding (03/2005)

[H.323] - Packet-based multimedia communications systems (06/2006)

[H.350] - Directory services architecture for multimedia conferencing (08/2003)

[H.350.1] - Directory services architecture for H.323 (08/2003)

[H.350.2] - Directory services for H.235 (08/2003)

[H.350.3] - Directory service architecture for H.320 (08/2003)

[H.350.4] - Directory services architecture for SIP (08/2003)

[H.350.5] - Directory services architecture for non-standard protocols (08/2003)

[H.350.6] - Directory services architecture for call forwarding and preferences (03/2004)

[H.350.7] - Directory services architecture for XMPP (01/2007)

[H.450.1] - Generic functional protocol for the support of supplementary services in H.323 (02/1998)

[H.450.2] - Call transfer supplementary service for H.323 (02/1998)

[H.450.3] - Call diversion supplementary service for H.323 (02/1998)

[H.450.4] - Call hold supplementary service for H.323 (05/1999)

[H.450.5] - Call park and call pickup supplementary services for H.323 + Erratum (May 2000) (05/1999 + Erratum 2000)

[H.450.6] - Call waiting supplementary services for H.323 (05/1999)

[H.450.7] - Message waiting indication supplementary service for H.323 (05/1999)

[H.450.8] - Name identification supplementary services for H.323 (02/2000)

[H.450.9] - Call completion supplementary services for H.323 (11/2000)

[H.450.10] - Call offering supplementary service for H.323 (03/2001)

[H.450.11] - Call intrusion supplementary service for H.323 (03/2001)

[H.450.12] - Common Information additional Network Feature for H.323 (07/2001)

[H.460.1] - Guidelines for the use of the generic extensible framework (03/2002)

[H.460.2] - Number Portability internetworking between H.323 and SCN networks (07/2001)

[H.460.3] - Circuit maps within H.323 systems (11/2002)

[H.460.4] - Call priority designation and country/international network of call identification for H.323 priority calls (01/2007)

[H.460.5] - H.225.0 transport of multiple Q.931 information elements of the same type (11/2002)

[H.460.6] - Extended Fast Connect feature (11/2002)

[H.460.7] - Digit maps within H.323 systems (11/2002)

[H.460.8] - Querying for alternate routes within H.323 systems (11/2002)

[H.460.9] - Support for online QoS-monitoring reporting within H.323 systems (11/2002)

[H.460.10] - Call party category within H.323 systems (03/2004)

[H.460.11] - Delayed call establishment within H.323 systems (03/2004)

[H.460.12] - Glare control indicator within H.323 systems (03/2004)

[H.460.13] - Called user release control (03/2004)

[H.460.14] - Support for Multi-Level Precedence and Preemption (MLPP) within H.323 systems (03/2004)

[H.460.15] - Call signaling transport channel suspension and redirection within H.323 systems (03/2004)

[H.460.16] - Multiple message released sequence capability (01/2005)

[H.460.17] - Using H.225.0 call signaling connection as transport for H.323 RAS messages (09/2005)

[H.460.18] - Traversal of H.323 media across network address translators and firewalls (09/2005)

[H.460.19] - Traversal of H.323 media across network address translators and firewalls (09/2005)

[H.460.20] - Location number within H.323 systems (09/2005)

[H.460.21] - Message broadcast for H.323 systems (05/2006)

[H.460.22] - Negotiation of security protocols to protect H.225.0 Call Signaling Messages (01/2007)

[H.501] - Protocol for mobility management and intra/inter-domain communication in multimedia systems (03/2002)

[H.510] - Mobility for H.323 multimedia systems and services (03/2002)

[H.530] - Symmetric security procedures for H.323 mobility in H.510 (03/2002)

[T.37] - Procedures for the transfer of facsimile data via store-and-forward on the Internet (06/1998)

[T.38] - Procedures for real-time Group 3 facsimile communication over IP networks (09/2005)

[T.122] - Multipoint communication service - Service definition (02/1998)

[T.124] - Generic conference control (02/1998)

[T.125] - Multipoint Communication Service Protocol (MCS) (02/1998)

[T.126] - Multipoint still image and annotation protocol (07/1997)

[T.127] - Multipoint binary file transfer protocol (08/1995)

[X.224] - Information technology - Open Systems Interconnections - Protocol for providing the connection-mode transport service (11/1995)

(1) n.i. BO.