ATIS-1000010.2006(R2011)

SUPPORT OF EMERGENCY TELECOMMUNICATIONS SERVICE (ETS) IN IP NETWORKS

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to the validity of this claim or any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher.

ATIS-1000010.2006, *Support of Emergency Telecommunications Service (ETS) in IP Networks*

Is an American National Standard developed by the **Signaling, Architecture, and Control (SAC) Subcommittee** under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000010.2006

American National Standard for Telecommunications

SUPPORT OF EMERGENCY TELECOMMUNICATIONS SERVICE (ETS) IN IP NETWORKS

Secretariat

Alliance for Telecommunications Industry Solutions

Approved June 12, 2006

American National Standards Institute, Inc.

Abstract

This document defines the procedures and capabilities required to support Emergency Telecommunications Service (ETS) within and between Internet Protocol (IP) based service provider networks.

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) -- formerly T1S1 -- develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC, which is responsible for the development of this Standard, had the following members:

R. Hall, PTSC Chair
J. Zebarth, PTSC Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
M. Dolly, PTSC Technical Editor

Organization Represented	Name of Representative
AcmePacket	Kevin Klett
Alcatel USA Inc.	Ken Biholar
AT&T	Bob Hall George Stanek (Alt.)
BellSouth Telecommunications	Rick McNealy
C.S.I Telecommunications	Michael S. Newman Thomas G. Croda (Alt.)
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt.)
Cisco Systems	Rajiv Kapoor Mike Hammer (Alt.)
Defense Info. Systems Agency	Chris Fitzgerald Ryan Kuseski (Alt.)
Ericsson Incorporated	Susana Sabater-Maroto Stephen Hayes (Alt.)
FBI ESTS	Robert Holman Edward Ignacio (Alt.)
Harris Corporation	Marlis Humphrey
Hewlett-Packard	Steve Mills
Intelsat	Mark T. Neibert
Lucent Technologies	Stuart O. Goldman

Organization Represented	Name of Representative
National Communications System	Nicholas Andre Carol-Lyn Taylor (Alt.)
NeuStar	Chris Celiberti
Nokia Telecommunications	Joyabrata Mukherjee Ed Ehrlich (Alt.)
Nortel Networks	Joseph A. Zebarth
Qwest	Steve Showell Michael Fargano (Alt.)
Siemens Info & Comm Ntwks, Inc.	Ron Franks David E. Francisco (Alt.)
Sprint LTD	Jack Mooningham
Sprint Nextel	Mark L. Jones
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt.)
Tellabs Operations, Inc.	William A. Walker
Tridea Works	Greg Ratta
VeriSign, Inc.	Anthony M Rutkowski
Verizon Communications	Thomas Helmes Christine Huff (Alt.)

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard for Telecommunications –

Support of Emergency Telecommunications Service (ETS) in IP Networks

1 INTRODUCTION

This document defines the procedures and capabilities required to support Emergency Telecommunications Service (ETS) within and between Internet Protocol (IP) based service provider networks. It also includes:

- Procedures for interoperability/interworking between IP-based and existing circuit-switched wireline and wireless service provider networks;
- Basic ("GETS-like") authentication mechanisms and procedures; and
- Security requirements.

ETS is a forward-looking service that requires priority treatment in the IP network infrastructure in support of National Security/Emergency Preparedness (NS/EP) communications. ETS has capabilities to increase the probability of successful completion of calls, sessions, or other communications initiated by government authorized users over the public network infrastructure. ETS also includes legacy circuit-switched NS/EP services such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS)[1].

This document includes end-to-end ETS call flows that illustrate calls originating and terminating on:

- IP access (e.g., cable or DSL);
- narrowband wireline access (e.g., POTS phone); and
- wireless access (e.g., GSM or CDMA phone);

that traverse through IP and circuit-switched Core Networks. A service description of ETS is contained in the ATIS Technical Report (TR), *Service Description of ETS* [ANSI-1000005]. The ETS and WPS procedures previously defined for circuit-switched wireline [ANSI-1000006.2005] and wireless [ANSI TIA-917, 3GPP TR 22.952] technologies, respectively, are not impacted by this document.

[1] TIA uses the term "Wireless Priority Service," whereas 3GPP uses the term "Priority Service".

2 ABBREVIATIONS & ACRONYMS

ANSI	American National Standards Institute
AS	Application Server
CCFE	Call Control Functional Entity
CDMA	Code-Division Multiple Access
CPC	Calling Party's Category
ETS	Emergency Telecommunications Service
ets.x	RPH name space for ETS with priority value x
GETS	Government Emergency Telecommunications Service
GSM	Global System for Mobile Communications
IAM	Initial Address Message
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated-Services Digital Network
ISTP	Internet Signaling Transport Protocol
ISUP	ISDN User Part
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MS	Media Server
MS	Mobile Station
MSC	Mobile Switching Center
MTP	Message Transfer Part
NNI	Network to Network Interface
NS/EP	National Security/Emergency Preparedness
P-CSCF	Proxy Call Session Control Function
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
RPH	Resource Priority Header
S-CSCF	Serving Call Session Control Function
SIP	Session Initiation Protocol
SS7	Signaling System No. 7
TDM	Time Division Multiplexing
TIA	Telecommunications Industry Association
TR	Technical Report
WPS	Wireless Priority Service
wps.y	RPH name space for WPS with priority value y
WPS-FC	Wireless Priority Service Feature Code

3 NORMATIVE REFERENCES

3.1 ANSI references

T1.673-2002 (R2007), *BICC Capability Set 1+*.[2]

T1.679-2004, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*.[2]

ATIS-1000005, *Service Description of ETS*.[2]

ANSI-1000006.2005, *Signalling System No. 7 (SS7) – Emergency Telecommunications Service (ETS)*.[2]

ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.[2]

ATIS-100009.2006, *IP Network-to-Network Interface (NNI) Standard for VoIP*.[2]

ANSI TIA-917, *Wireless Priority Service Enhancements for CDMA Systems*.[3]

3.2 ITU

ITU-T Recommendation X.805 (10/03), *Security architecture for systems providing end-to-end communications*.[4]

ITU-T G.711, *Pulse Code Modulation (PCM) of Voice Frequencies*.[4]

3.3 IETF references[5]

IETF RFC 1321, *The MD5 Message-Digest Algorithm*.

IETF RFC 2246, *The TLS Protocol Version 1.0*.

IETF RFC 2429, *RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)*.

IETF RFC 4566, *SDP: Session Description Protocol*.

IETF RFC 2401, *Security Architecture for the Internet Protocol*.

IETF RFC 4733, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

IETF RFC 3261, *SIP: Session Initiation Protocol*.

IETF RFC 3262, *Reliability of Provisional Responses in Session Initiation Protocol (SIP)*.

---

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[3] This document is available from the Telecommunications Industry Association (TIA). < http://www.tiaonline.org/standards/overview.cfm >

[4] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[5] These documents are available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

IETF RFC 3263, *Session Initiation Protocol (SIP): Locating SIP Servers*.

IETF RFC 3264, *An Offer/Answer Model with the Session Description Protocol (SDP)*.

IETF RFC 3265, *Session Initiation Protocol (SIP)-Specific Event Notification*.

IETF RFC 3311, *The SIP UPDATE Method*.

IETF RFC 3312, *Integration of Resource Management and Session Initiation Protocol (SIP)*.

IETF RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.

IETF RFC 3324, *Short Term Requirements for Network Asserted Identity*.

IETF RFC 3325, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.

IETF RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP)*.

IETF RFC 3428, *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

IETF RFC 3489, *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

IETF RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*.

IETF RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*.

IETF RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*.

IETF RFC 3581, *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Handling*.

IETF RFC 3711, *The Secure Real-time Transport Protocol (SRTP)*.

IETF RFC 3725, *Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)*.

IETF RFC 3824, *Using E.164 numbers with the Session Initiation Protocol (SIP)*.

IETF RFC 3842, *A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)*.

IETF RFC 3856, *A Presence Event Package for the Session Initiation Protocol (SIP)*.

IETF RFC 3857, *Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)*.

IETF RFC 3858, *An Extensible Markup Language (XML) Based Format for Watcher Information*.

IETF RFC 3859, *Common Profile for Presence (CPP)*.

IETF RFC 3860, *Common Profile for Instant Messaging (CPIM)*.

IETF RFC 3861, *Address Resolution for Instant Messaging and Presence*.

IETF RFC 3862, *Common Presence and Instant Messaging (CPIM): Message Format*.

IETF RFC 3863, *Presence Information Data Format (PIDF)*.

IETF RFC 3891, *The Session Initiation Protocol (SIP) "Replaces" Header*.

IETF RFC 3892, *The Session Initiation Protocol (SIP) Referred-By Mechanism*.

IETF RFC 3903, *Session Initiation Protocol (SIP) Extension for Event State Publication*.

IETF RFC 3959, *The Early Session Disposition Type for the Session Initiation Protocol (SIP)*.

IETF RFC 3960, *Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)*.

IETF RFC 3966, *The tel URI for Telephone Numbers*.

IETF RFC 3994, *Indication of Message Composition for Instant Messaging*.

IETF RFC 4028, *Session Timers in the Session Initiation Protocol (SIP)*.

IETF RFC 4244, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.

IETF RFC 4504, *SIP Telephony Device Requirements and Configuration*.

IETF RFC 4568, *Session Description Protocol (SDP) Security Descriptions for Media Streams*.

IETF RFC 4458, *Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)*.

IETF RFC 4480, *RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)*.

IETF RFC 4629, *RTP Payload Format for ITU-T Rec. H.263 Video*.

IETF RFC 4662, *A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists*.

IETF RFC 4579, *Session Initiation Protocol Call Control - Conferencing for User Agents*.

IETF RFC 4575, *A Session Initiation Protocol (SIP) Event Package for Conference State*.

IETF RFC 4730, *A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)*.

IETF RFC 4961, *Symmetric RTP/RTP Control Protocol (RTCP)*.

draft-ietf-simple-partial-pidf-format-08, *Presence Information Data format (PIDF) Extension for Partial Presence*, November 2006.

draft-ietf-mmusic-ice-15, *Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Multimedia Session Establishment Protocols*, September 2007.

3.3.1 Call Control Signaling

IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*.

IETF RFC 2327 (1998), *SDP: Session Description Protocol*.

IETF RFC 2806 (2000), *URLs for Telephone Calls*.

IETF RFC 2976 (2000), *The SIP INFO Method*.

IETF RFC 3087, *Control of Service Context using SIP Request-URI*.

IETF RFC 3204 (2001), *MIME media types for ISUP and QSIG Objects*.

IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.

IETF RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.

IETF RFC 3324, *Short Term Requirements for Network Asserted Identity*.

IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.

IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP)*.

IETF RFC 3398, *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*.

IETF RFC 3420, *Internet Media Type message/sipfrag*.

IETF RFC 3428, *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

IETF RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*.

IETF RFC 3824, *Using E.164 numbers with the Session Initiation Protocol (SIP)*.

IETF RFC 3891, *The Session Initiation Protocol (SIP) "Replaces" Header*.

IETF RFC 3892, *The SIP Referred-By Mechanism*.

IETF RFC 3893, *SIP Authenticated Identity Body (AIB) Format*.

IETF RFC 3911, *The Session Initiation Protocol (SIP) "Join" Header*.

IETF RFC 3959, *The Early Session Disposition Type for the SIP*.

IETF RFC 3960, *Early Media and Ringback Tone Generation in the Session Initiation Protocol*.

IETF RFC 3966, *The tel URI for Telephone Calls*.

IETF RFC 4028, *Session Timers in SIP*.

IETF RFC 4412, *Communications Resource Priority for the Session Initiation Protocol (SIP)*.

draft-ietf-iptel-trunk-group-06.txt, *Representing Trunk Goups in tel/sip URIs* (status: stable- AD watching).

draft-ietf-iptel-tel-np-08.txt, *New Parameters for the "tel" URI to Support Number Portability* (status: stable- AD Evaluation).

3.3.2 Media references

IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

IETF RFC 3267 (2002), *Real-time Transport Protocol RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs*.

IETF RFC 3389 (2002), *RTP Payload for Comfort Noise*.

IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control*.

3.4 Other

3GPP TR 22.952, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Priority service guide; (Release 6)*.[6]

4 FUNCTIONAL REFERENCE MODEL

Figure 1 illustrates the functional reference model for the support of ETS in IP networks. This is the same model as used for the IP-IP NNI between two interconnecting service providers. It consists of a signaling interface and a bearer interface. The signaling and bearer interfaces support the flow of information among the following IP network logical entities: *Call Routing Functional Entity (CRFE)*, *Call Control Functional Entity (CCFE)*, and *Bearer Functional Entity (BFE)*, as defined in ATIS-1000009.2006. In support of ETS in IP networks, the ETS specific information (e.g., ETS call marking, calling user's priority level) needs to be signaled across the IP-IP NNI between two interconnecting VoIP providers. Support of the end-to-end ETS service requires the interworking of ETS specific information between the IP technology domain and other technology domains (e.g., wireless or wireline TDM domains).

[6] This document is available from the Third Generation Partnership Project (3GPP) at
< http://www.3gpp.org/specs/specs.htm >.

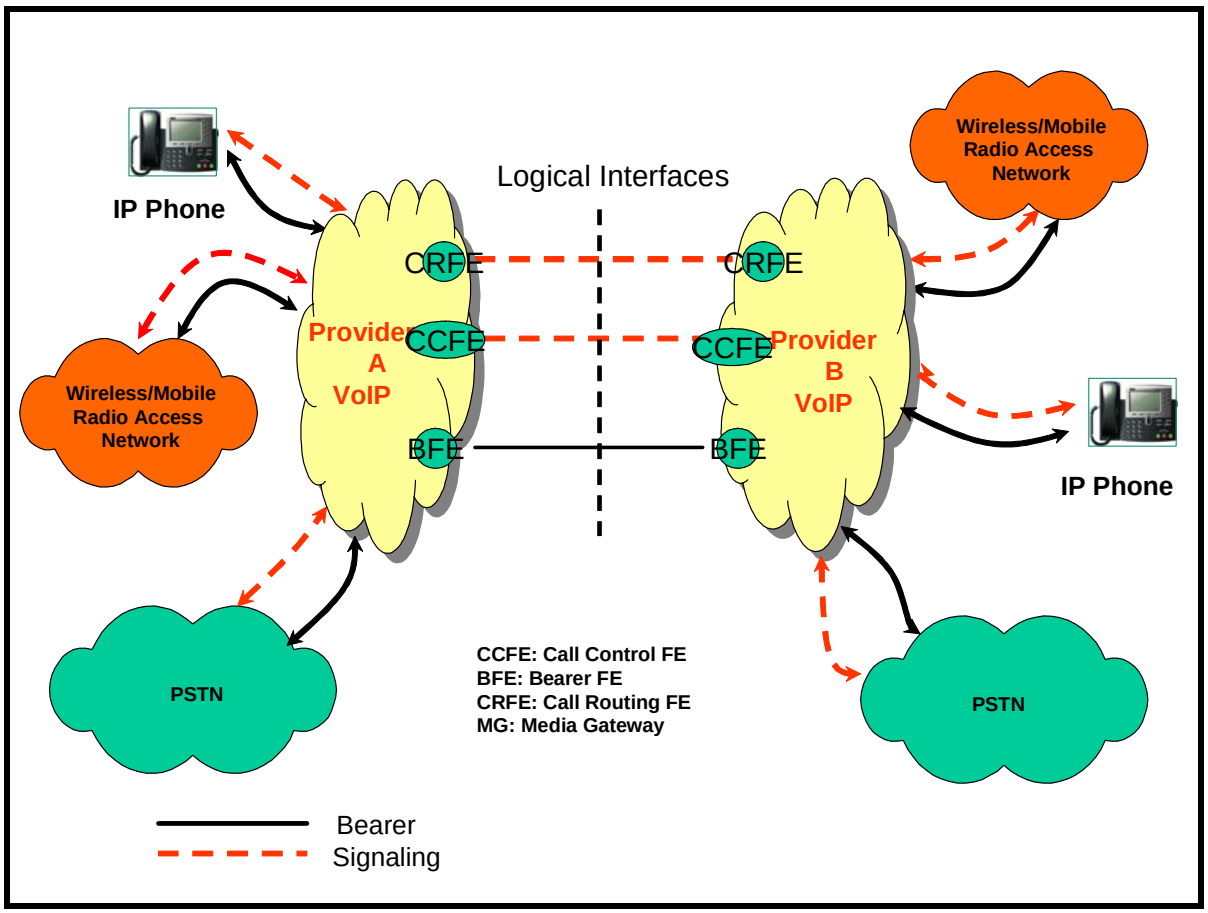

Figure 1 - ETS in IP Networks Reference Model

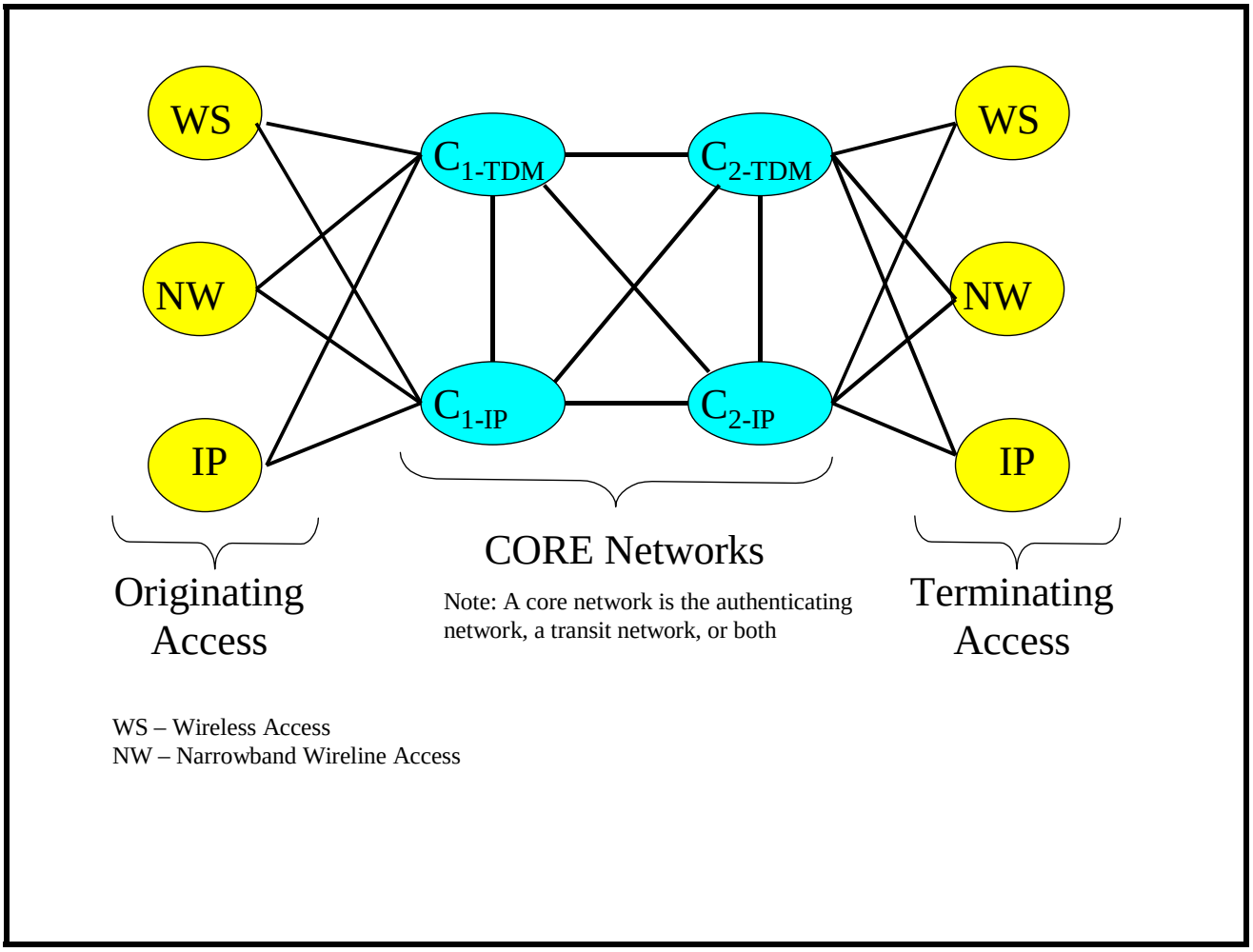

Figure 2 - End-to-End Call Matrix

Figure 2 is an end to end call matrix for the call flows illustrated in this document. It illustrates calls:

- Originating and terminating on IP (e.g., Cable and DSL), narrowband wireline (e.g., POTS phone), and wireless (e.g., GSM and CDMA phone) access; and
- Traversing through IP and circuit-switched (TDM) Core Networks.

The call/session scenarios associated with Figure 2 can be found in clause 6.

An ETS call may be initiated by dialing an ETS-specific DN, called *ETS-DN* in this standard. A WPS call is a call dialed using a *WPS-Feature Code (WPS-FC)*. A WPS call is treated as a specific type of ETS call.

When the calling party dials a WPS-FC+ETS-DN, the call is treated both as a WPS call and an ETS call. In particular, the call is subject to both WPS and ETS authentication.

5 EMERGENCY TELECOMMUNICATIONS SERVICE IN IP NETWORKS

5.1 Assumptions and General Principles

5.1.1 Assumptions

1. Within an IP domain, an ETS call/session is assigned one of five user priority levels associated with the calling service user.
2. SIP messages are only processed by SIP proxies/UAs, and therefore the SIP Resource Priority Header (RPH) is not processed by IP transport elements (e.g., routers).
3. Two types of core networks are considered in this standard: *IP* and *TDM*.
4. Three different originating and terminating access types are considered in this standard: *wireline IP* (e.g., DSL, cable), *wireline TDM*, and *wireless*.
5. An NS/EP call/session can traverse multiple IP and TDM core networks.
6. An ETS call originating over an IP access is authenticated either in an IP or a TDM core network. A WPS call is authenticated by the wireless service provider network of the calling party. IP-based wireless authentication (e.g., for UMTS) is not addressed in this document.
7. If both WPS and ETS authentication occur (i.e., the calling user dials WPS-FC+ETS-DN), the WPS authentication -- at the wireless access -- occurs before the ETS authentication.
8. If the authentication process identifies a user priority, both the ets and wps namespaces may be set to the same priority values. The wps namespace reflects the actual user priority.
9. The service provider's managed access and core networks are secure.
10. The DTMF tones are carried across an IP core network in accordance with RFC 4733, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

5.1.2 General Principles

1. Two types of authentication functions are considered in this document.
    - ***ETS authentication*** – This type of authentication is invoked when the calling user dials an ETS-DN.
        i. *If the call is authenticated in the TDM domain*, after the call is authenticated:
            - The CPC parameter in the IAM is set to "NS/EP Call."
            - Existing TDM authentication mechanisms do not have the calling user's priority value, so the Precedence parameter is not included in the IAM. If future authentication mechanisms have the calling user's priority value, the Precedence parameter will be included in the IAM.
        ii. *If the call is authenticated in the IP domain*, after the call is authenticated:
            - If the calling user's priority level is not available, only ets.x is created in the RPH, where x is a default priority value based on policy; or
            - If the calling user's priority level is available, both ets.x and wps.y namespaces are created in the RPH, where y is the calling user's priority level and x is based on policy.
    - ***WPS authentication*** – This type of authentication is invoked when the calling user dials a WPS-FC+DN.

i. *If the call is authenticated in the TDM domain*, after the call is authenticated:
   - The CPC parameter in the IAM is set to "NS/EP Call."
   - If the calling user's priority level is available, the Precedence level (in the Precedence parameter) in the IAM would also be set (precedence level 0 – 4 corresponding to user priorities 1 – 5).

ii. *WPS authentication in the IP domain* (e.g., for UMTS phones) is not addressed in this document.

Successful ETS authentication may result in changing the priority values in the ets or wps namespaces.

2. The ets priority level (x) of an ETS (including a WPS) call/session is carried in the SIP RPH namespace, "ets.x", where x=4 to 0, where 0 is the highest priority.
   - *For a call traversing from a circuit-switched network to an IP network*, the Ingress IP Gateway (IIP-GW) creates the SIP RPH ets namespace based on the presence of ETS-DN in the Called Party Number parameter, or the Calling Party's Category parameter coded as "NS/EP Call" in the received IAM. The IIP-GW assigns the ets priority level. It is mandatory for the IIP-GW to support a provisionable default value for the ets priority level. The default value for the ets priority level is determined by policy[7]. If no ISUP Precedence parameter is received, the default value is used to populate the ets priority level. If a Precedence parameter is received, then, based on policy, either the default value or the precedence level in the Precedence parameter is used to populate the ets priority level.
   - *An ETS Authentication Application Server (AS)* may modify the value of the received ets priority level based on a successful Authentication Verification Processing. An ETS Authentication AS deletes the received RPH if the authentication is denied.
3. A successfully authenticated WPS call/session includes the RPH with the ets namespace. In addition to the ets.x, the RPH for a successfully authenticated WPS call/session contains the "wps.y" namespace with the priority level (y) associated with the calling WPS user. For a WPS call/session traversing from a circuit-switched network to an IP network, the IIP-GW maps the precedence level in the received Precedence parameter to the priority value in the wps namespace. The precedence level is determined during authentication of the WPS user.The presence of the ets namespace indicates an ETS or a WPS call/session and triggers priority treatment. However, the priority value (x) in the "ets.x" may be used for priority treatment only in the IP domain and is not used for priority treatment on the wireless access. The wps namespace value (y) is used for priority treatment on the wireless access.
4. The wps.y namespace is transported through the IP domain to facilitate priority treatment on the wireless access.
   - *An ETS Authentication Application Server (AS)* may modify a received wps priority level, or -- if a wps namespace is not received -- create a wps namespace based on Authentication Verification Processing.
   - *For a call traversing from an IP network to a circuit-switched network*, the Egress IP Gateway (EIP-GW) shall use the priority level in the wps namespace, if present, to populate the precedence level of the Precedence parameter in the outgoing ISUP IAM.

[7] The policy will be determined by the NCS. The same policy will be applicable to all concerned service providers in a given scenario.

- *For a call traversing from an IP network to a circuit-switched network*, if the ets.x namespace is present but the wps.x namespace is not present, the EIP-GW shall not send the Precedence parameter in the outgoing ISUP IAM.

5. Processing of ETS calls/sessions, including the associated signaling and media, are provided priority treatment over non-ETS calls based on the presence of ets.x.
6. The ets.x RPH priority value may be used for priority treatment of ETS traffic at certain interfaces, such as IP access-to-core and IP network-to-network interfaces, where connection admission control may be applied.
7. The ets.x RPH priority value may be used by SIP proxies and B2BUAs to make routing decisions, particularly on IP access.
8. Based on policy, the Session Border Control function (CCFE and BFE) facing a user may modify a received RPH ets priority level with the provisioned default value.
9. All packets associated with an ETS call/session must receive priority handling:
   i. In network element queues,
   ii. For access to the IP backbone, and
   iii. Within the IP backbone.

   This priority handling is based on the presence of an ets namespace in an RPH.
10. A secure mechanism that validates the identity of the far end sending network is required in order to support priority handling of packets on an IP-NNI.

5.2 Protocol Behavior

The procedures in this document only apply to supporting ETS in IP Access and Core Networks, including interworking with circuit-switched systems. The ETS and WPS procedures previously defined for circuit-switched wireline [ANSI-1000006.2005] and wireless [ANSI TIA-917] technologies respectively are not impacted by this document, and therefore will only be referenced.

5.2.1 Protocol Mappings

5.2.1.1 ISUP to SIP Mappings

Table 1 shows the mapping from ISUP to SIP for ETS related information.

Table 1 - ISUP to SIP Mappings

ISUP	SIP
CdPN = Destination Number CPC not equal to NS/EP Call No PRECEDENCE PARAMETER This is a normal (non-ETS) call	R-URI/To: = Destination Number
CdPN = ETS-DN CPC = NS/EP Call No PRECEDENCE PARAMETER	R-URI/To: = ETS-DN RPH [ets.DF]
CdPN = Destination Number CPC = NS/EP Call No PRECEDENCE PARAMETER	R-URI/To: = Destination Number RPH [ets.DF]
CdPN = ETS-DN CPC not equal to NS/EP Call No PRECEDENCE PARAMETER	R-URI/To: = ETS-DN RPH [ets.DF]
CdPN = Destination Number CPC not equal to NS/EP Call PRECEDENCE PARAMETER = Look Ahead for Busy = 10 Precedence Level = y (0 – 4) Network Identity = 0100 MLPP Service Domain = z (H'40024B' - H'40024F') This is an errored header	Request for ETS handling is rejected, and the call is processed as an ordinary call.
CdPN = Destination Number CPC = NS/EP Call PRECEDENCE PARAMETER = Look Ahead for Busy = 10 Precedence Level = y (0 – 4) Network Identity = 0100 MLPP Service Domain = z (H'40024B' - H'40024F')	R-URI/To: = Destination Number RPH [ets.DF or ets.y, wps.y]

CdPN = ETS-DN CPC = NS/EP Call PRECEDENCE PARAMETER = Look Ahead for Busy = 10 Precedence Level = y (0 – 4) Network Identity = 0100 MLPP Service Domain = z (H'40024B' - H'40024F')	R-URI/To: = ETS-DN RPH [ets.DF or ets.y, wps.y]
CdPN = ETS-DN CPC not equal to NS/EP Call PRECEDENCE PARAMETER = Look Ahead for Busy = 10 Precedence Level = y (0 – 4) Network Identity = 0100 MLPP Service Domain = z (H'40024B' - H'40024F') This is an errored header	R-URI/To: = ETS-DN RPH [ets.DF, wps.y]
The default (DF) priority level is provisioned at the PSTN Gateway and its value is determined by policy. The default priority level is used until the call can be authenticated. The NS/EP Call value for CPC is H'E2'. Note that if y = 0 then z = H'40024B', and if y = 4 then z = H'40024F'.	

5.2.1.2 SIP to ISUP Mappings

Table 2 shows the mapping from SIP to ISUP for ETS related information.

Table 2 - SIP to ISUP Mappings

SIP	ISUP
R-URI/To: = Destination Number This is a normal (non-ETS) call	CdPN = Destination Number CPC not equal to NS/EP Call MTP PRIORITY = 0 No PRECEDENCE PARAMETER
R-URI/To: = Destination Number RPH [ets.x]	CdPN = Destination Number CPC = NS/EP Call, MTP PRIORITY = 1 No PRECEDENCE PARAMETER
R-URI/To: = Destination Number RPH [ets.x, wps.y]	CdPN = Destination Number CPC = NS/EP Call, MTP PRIORITY = 1 PRECEDENCE PARAMETER = Look Ahead for Busy = 10 Precedence Level = y (0 – 4) Network Identity = 0100 MLPP Service Domain = z (H'40024B' - H'40024F')
R-URI/To: = ETS-DN No RPH or ets.DF	CdPN = ETS-DN CPC = NS/EP Call, MTP PRIORITY = 1 No PRECEDENCE PARAMETER
R-URI/To: = ETS-DN RPH [ets.x, wps.y]	CdPN = ETS-DN CPC = NS/EP Call, MTP PRIORITY = 1 PRECEDENCE PARAMETER = Look Ahead for Busy = 10 Precedence Level = y (0 – 4) Network Identity = 0100 MLPP Service Domain = z (H'40024B' - H'40024F')
R-URI/To: = ETS-DN RPH [wps.y] This is an errored header	Request is rejected.

R-URI/To: = Destination Number RPH [wps.y] This is an errored header	Request is rejected.
The default (DF) priority level is provisioned at the PSTN Gateway and its value is determined by policy. The default priority level is used until the call can be authenticated. The NS/EP Call value for CPC is H'E2'. Note that if y = 0 then z = H'40024B', and if y = 4 then z = H'40024F'.	

5.2.2 ETS SIP Procedures

The following SIP messages *shall* contain an RPH for recognized ETS calls/sessions:

- INVITE [RFC 3261]
- ACK [RFC 3261]
- BYE [RFC 3261]
- CANCEL [RFC 3261]
- INFO [RFC 2976]
- MESSAGE [RFC 3428]
- NOTIFY [RFC 3265]
- OPTIONS [RFC 3261]
- PRACK [RFC 3262]
- PUBLISH [RFC 3903]
- REFER [RFC 3515]
- REGISTER [RFC 3261]
- SUBSCRIBE [RFC 3265]
- UPDATE [RFC 3311]

The RPH must also be contained in 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses associated with recognized ETS calls/sessions, with the exception of 401, "unauthorized".

A SIP request with a RPH is provided priority treatment by SIP elements (UAs, proxies, back-to-back UAs). The following are potential examples of such priority treatment in the SIP elements:

- SIP elements may override restrictive network capacity controls.
- SIP elements may provide enhanced routing functions.
- SIP elements may queue a request that cannot be processed due to a lack of resources.
- SIP elements may provide priority access to processing resources.

A SIP INVITE with an RPH is given priority for access to PSTN gateway resources such as trunks via trunk queuing when all trunks are busy. A PSTN gateway exempts ETS calls from restrictive network management controls that may be applicable to non-ETS calls. Also, the gateway maps RPH

information to appropriate ISUP indications (NS/EP call indication and priority level, as in 5.2.1.2) to facilitate providing priority treatment in the PSTN.

The presence of the RPH influences priority handling in network element queues, access to the IP backbone, and within in the IP backbone.

According to the normal rules of RFC 3261, Section 8.2.2, if a UAS does not understand the RPH field in a request, the server must ignore that header field, continue processing the message, and propagate the RPH downstream unchanged.

5.3 Authentication Procedures

This clause describes authentication procedures within an IP network. With the exception of the Application Server and the Media Server, the authentication procedures are architecture agnostic.

For the authentication procedures in this clause, it is assumed that the calling user's priority level is not available to the ETS AS. Therefore, only the ets namespace is created in the RPH after successful authentication; the wps namespace is not created in the RPH.

The prompt and collect instructions will be encoded in XML/VXML schema that is either transported with http(s) or SIP INFOs.

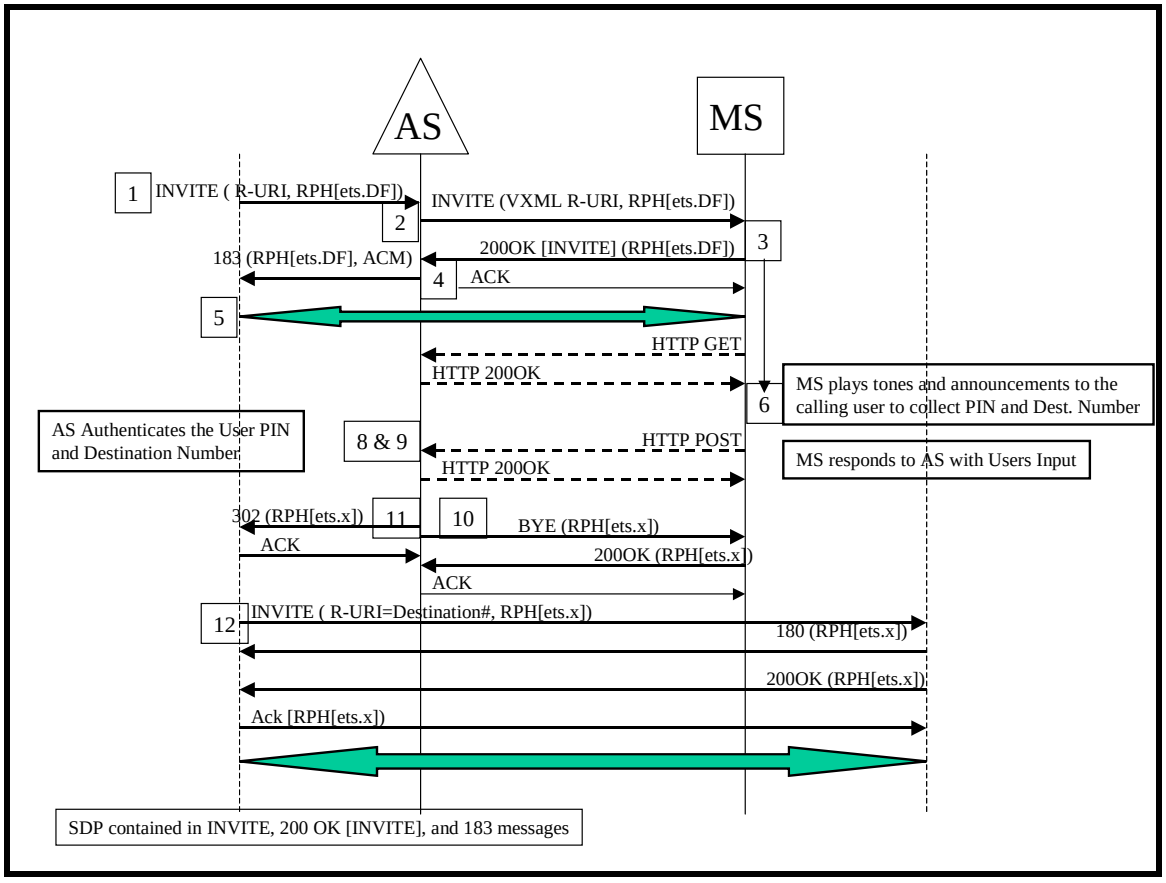

Figure 3 – Prompt & Collect Authentication, with VXML

Figure 3 illustrates a Basic ("GETS-like") ETS-user authentication. The calling user dials an ETS-DN.

1. The call/session is routed to an ETS Application Server (AS) where user authentication processing is initiated. The R-URI contains the ETS-DN.
2. The AS sends an INVITE message to the Media Server (MS), with an SDP offer associated with the caller. The INVITE message contains the URL of a VoiceXML script, stored on the AS. The script describes how the MS should interact with the caller (what announcement to play, how to collect digits, how many digits to collect, interdigit timers, etc…).
3. Upon receipt of the INVITE message the MS:
    a. May send a 100 Trying to the AS (not shown).
    b. Retrieves the VoiceXML script directly from the AS using HTTP and the URL in the INVITE message. (MS sends a HTTP GET to the AS and VoiceXML script is returned from the AS in an HTTP 200 OK).
    c. Validates the script.
    d. Formulates and sends a 200 OK message containing its own SDP to the AS.
4. The AS sends a 183 including the session information it received from the MS to establish an early media connection between the caller and the MS.
5. At this point, the media connection is available between the MS and the Calling Party.
6. Upon receipt of the ACK and HTTP 200 OK, the MS executes the VoiceXML script. It plays a tone and collects the PIN (authorization code) entered by the caller (either DTMF or Voice input).
7. The MS then sends the collected digits (PIN) directly to the AS using an HTTP POST message
8. Upon receipt of the collected digits, the AS verifies whether the received digits (Authorization code) are valid.
    - *If the digits received are invalid (number of digits received or the wrong number)*, the AS determines that further interaction with the caller is required. The AS returns an HTTP 200 OK message to the MS with a new VoiceXML script. The AS will instruct for final handling treatment.
    - *If the received digits are valid*, the AS will instruct the MS to play the announcement to collect the digits (Destination Number).
9. The AS determines that the caller entered Destination digits are valid
10. The AS releases the MS from the call/session with a SIP BYE.
11. The AS sends a SIP 302, with a RPH that contains the priority set by the ETS AS.
12. The receiving element will use this RPH for all subsequent messaging and redirects the call/session towards the destination number.
13. The 200 OK from the destination network will include the SDP offer associated with the called party.

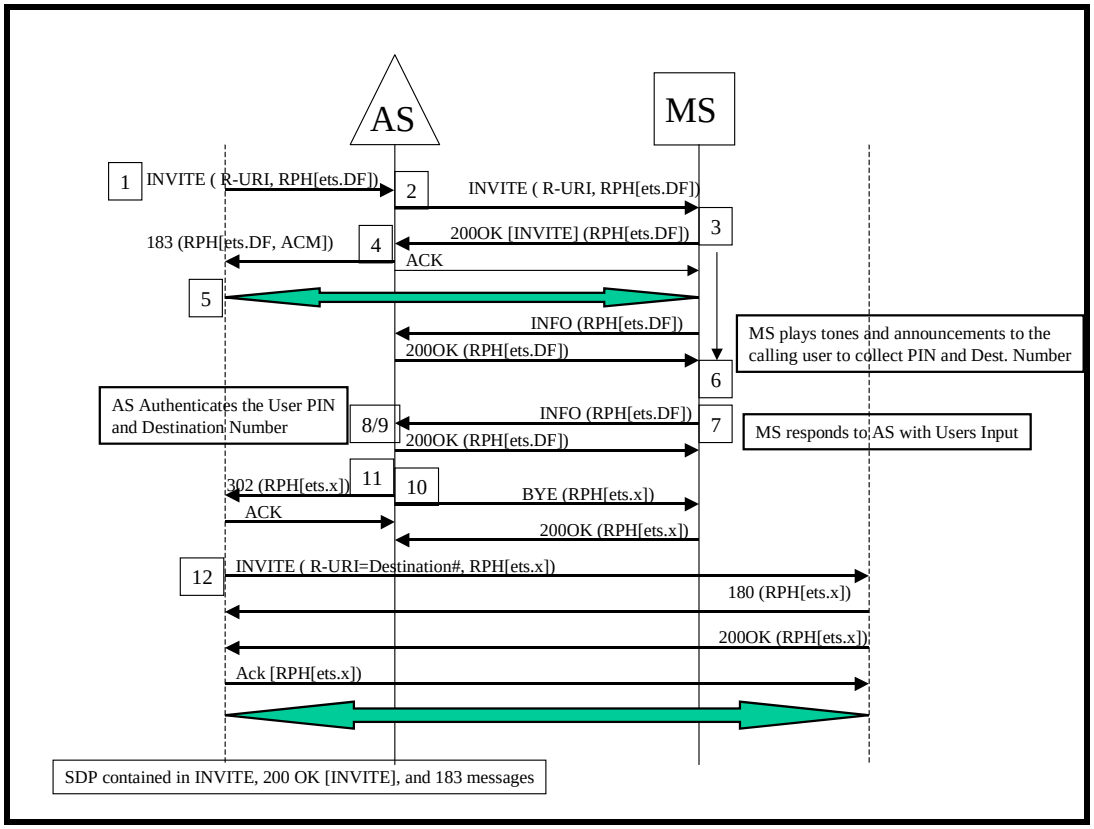

Figure 4 - Prompt & Collect Authentication, with SIP INFO [XML]

Figure 4 illustrates a call/session authentication similar to that in Figure 3 except that the XML scripts are included in SIP using SIP INFOs.

1. The call/session is routed to an ETS Application Server (AS) where user authentication processing is initiated.
2. The AS sends an INVITE message to the Media Server (MS), with an SDP offer associated with the caller.
3. Upon receipt of the INVITE message the MS:
   - ♦ May send a 100 Trying to the AS.
   - ♦ Retrieves the XML script directly from the AS using a SIP INFO message containing a request.
   - ♦ Validates the script.
   - ♦ Formulates and sends a 200 OK message containing its own SDP to the AS.
4. The AS sends a 183 to establish an early media connection with the caller, including in it the session information it received from the MS.
5. At this point, the media connection is available between the MS and the Calling Party.
6. Upon receipt of the ACK and SIP INFO with the XML script, the MS executes the XML script. It plays a tone and collects digits (authorization code) entered by the caller (either DTMF or Voice input).

7. The MS then sends the collected digits in an XML message transported in a SIP INFO message.
8. Upon receipt of the collected digits, the AS verifies whether the received digits (Authorization code) are valid.
   - *If the digits received are invalid (number of digits received or the wrong number)*, the AS determines that further interaction with the caller is required. The AS returns a SIP INFO message to the MS with a new XML instruction. The AS will execute the final handling treatment.
   - *If the received digits are valid*, the AS will instruct the MS to play the announcement to collect the digits (Destination Number).
9. The AS determines that the caller entered Destination digits are valid
10. The AS releases the MS from the call/session with a SIP BYE.
11. The AS sends a SIP 302, with a RPH that contains the priority set by the ETS AS.
12. The receiving network element will use this RPH for all subsequent messaging and redirects the call/session towards the destination number.

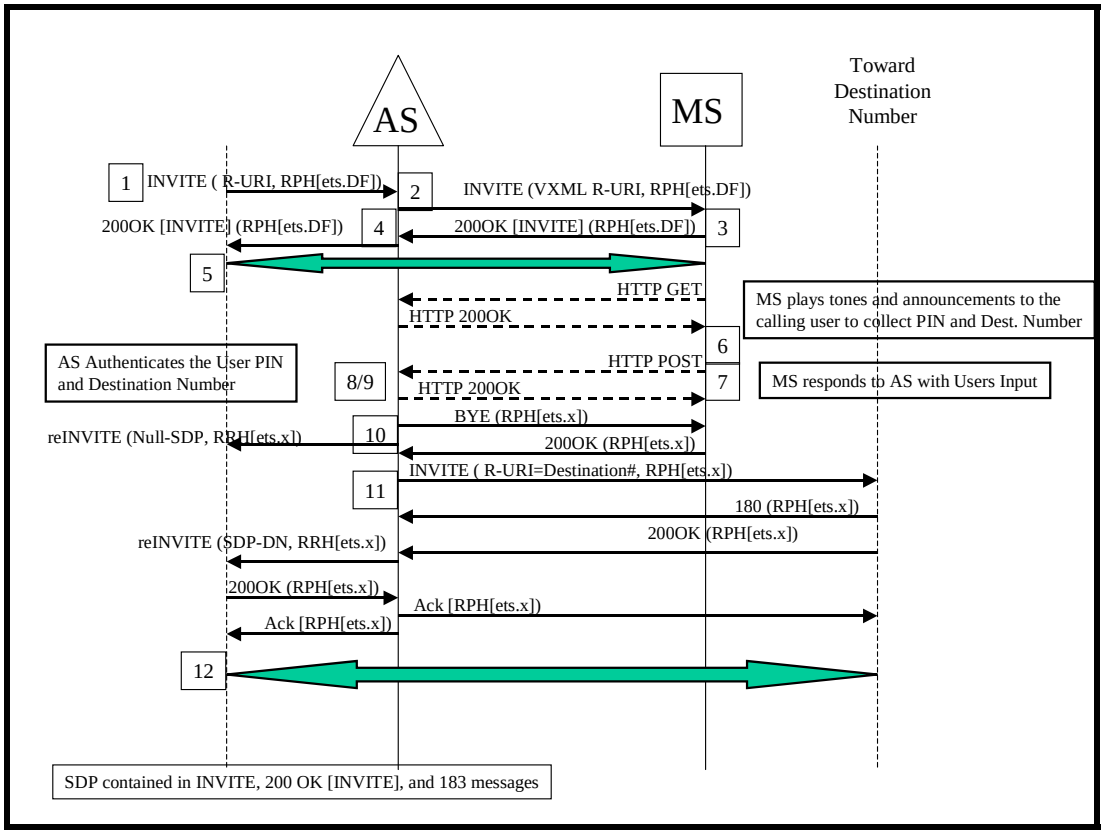

Figure 5 - Authenticating AS as a B2BUA

Figure 5 illustrates a Basic ("GETS-like") ETS-user authentication.

1. The call/session is routed to an ETS Application Server (AS) where user authentication processing is initiated.

2. The AS sends an INVITE message to the Media Server (MS), with an SDP offer associated with the caller. The INVITE message contains the URL of a VoiceXML script, stored on the AS. The script describes how the MS should interact with the caller (what announcement to play, how to collect digits, how many digits to collect, interdigit timers, etc…).
3. Upon receipt of the INVITE message the MS:
   - ♦ May send a 100 Trying to the AS.
   - ♦ Retrieves the VoiceXML script directly from the AS using HTTP and the URL in the INVITE message. (MS sends a HTTP GET to the AS and VoiceXML script is returned from the AS in an HTTP 200 OK).
   - ♦ Validates the script.
   - ♦ Formulates and sends a 200 OK message containing its own SDP to the AS.
4. The AS sends a 200 OK towards the calling party, including in it the session information it received from the MS.
5. At this point, the media connection is available between the MS and the Calling Party.
6. Upon receipt of the ACK and VXML script in the http 200 OK, the MS executes the VoiceXML script. It plays a tone and collects digits (authorization code) entered by the caller (either DTMF or Voice input).
7. The MS then sends the collected digits directly to the AS using an HTTP POST message
8. Upon receipt of the collected digits, the AS verifies whether the received digits (Authorization code) are valid.
   - ♦ *If the digits received are invalid (number of digits received or the wrong number)*, the AS determines that further interaction with the caller is required. The AS returns an HTTP 200 OK message to the MS with a new VoiceXML script. The AS will instruct for final handling treatment.
   - ♦ *If the received digits are valid*, the AS will instruct the MS to play the announcement to collect the digits (Destination Number).
9. The AS determines that the caller entered Destination digits are valid.
10. The AS releases the MS from the call/session with a SIP BYE, and sends a reINVITE toward the calling party, with a NULL-SDP to place the media on hold.
11. The AS sends an INVITE toward the destination party. Upon receiving 200 OK (answer), the AS sends a reINVITE with the SDP associated with the destination toward the calling party.
12. Media path is established between the calling party and destination number, with the authentication AS in the call control path as a B2BUA.

5.4 Call Processing Procedures

5.4.1 Originating Access to Core Network 1

5.4.1.1 Originating Wireline Access to IP Core Network

Illustrated call/session scenarios can be found in clause 6, flows A & B in Figure 9, and A & B in Figure 10.

Current call processing occurs at the originating wireline exchange. The following actions are taken at the PSTN-IP Gateway:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in the CdPN and/or CPC value of NS/EP Call.
2. Protocol interworking is performed as shown in Table 1.
3. The packets are priority marked, as defined in clause 8, and transmitted toward the IP Backbone, resulting in the packets receiving the highest priority treatment on access to the IP backbone and in the IP backbone.

5.4.1.2 Originating Wireless Access to IP Core Network

Illustrated call/session scenarios can be found in clause 6; flows C, D, & E in Figure 9; C & D in Figure 10, D in Figure 11; and C & D in Figure 13.

Current WPS call process is performed at the visited MSC or home system. The following actions are taken at the Wireless IP Gateway:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in the CdPN and/or CPC value of NS/EP Call.
2. Protocol interworking is performed as shown in Table 1.
3. The packets are priority marked, as defined in clause 8, and transmitted toward the IP Backbone, resulting in the packets receiving the highest priority treatment on access to the IP backbone and in the IP backbone.

5.4.1.3 Originating IP Access to IP Core Network

Illustrated call/session scenarios can be found in clause 6; flows A, B, & C in Figure 11.

The following actions are taken by the IP-IP Session Border Control function (core network's CCFE and BFE) interfacing the originating access:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in the R-URI and/or RPH with an ets namespace.
2. Based on policy:
   - *If no RPH is present*, an RPH may be populated with an ets namespace, with a priority level value of Default (DF).
   - *If an RPH is present with an ets namespace*, the priority level value may be reset to the DF.
3. The packets are priority marked, as defined in clause 8, and transmitted toward the IP Backbone, resulting in the packets receiving the highest priority treatment on access to the IP backbone and in the IP backbone

5.4.1.4 Originating IP Access to TDM Core Network

There are no illustrative examples for this scenario.

The following actions are taken at the IP-PSTN Gateway:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in the R-URI and/or RPH with an ets namespace.
2. Protocol interworking is performed as shown in Table 2.
3. Current TDM (circuit) priority call processing continues

5.4.2 Core 1 Network to Core 2 Network

Note that the two core networks may represent two service providers or a single service provider's domain.

5.4.2.1 TDM Core Network to IP Core Network

Illustrated call/session scenarios can be found in clause 6, flows A-D in Figure 8, and A-D in Figure 12.

Current call processing occurs on the originating wireline exchange. The following actions are taken at the PSTN Gateway:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in the CdPN and/or CPC value of NS/EP Call.
2. Validation of the identity of the far end sending network is not required. It is assumed that this validation occurred in the TDM core network, and that a trust relationship exists between the TDM core and the IP core.
3. Protocol interworking is performed as shown in Table 1.
4. The packets are priority marked, as defined in clause 8, and transmitted toward the IP Backbone, resulting in the packets receiving the highest priority treatment on access to the IP backbone and in the IP backbone.

5.4.2.2 IP Core Network to TDM Core Network

Illustrated call/session scenarios can be found in clause 6, flows A-D in Figure 9, and A & B in Figure 11.

The following actions are taken at the IP-PSTN Gateway:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in the R-URI and/or RPH with an ets namespace.
2. Validation of the identity of the far end sending network is not required. It is assumed that this validation occurred in the IP core network, and that a trust relationship exists between the IP core and the TDM core.
3. Protocol interworking is performed as shown in Table 2.
4. Current TDM (circuit) priority call processing continues.

5.4.2.3 IP Core 1 Network to IP Core 2 Network

Illustrated call/session scenarios can be found in clause 6, flows A-D in Figure 10, C & D in Figure 11, and A-D in Figure 13.

The following actions are taken at the IP-IP Session Border Control function (border CCFE and BFE of IP Core 2):

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of an ETS-DN in R-URI and/or RPH with ets namespace.
2. If there is not a trust relationship between IP core 1 and IP core 2, validation of the identity of the far end sending network occurs prior to proceeding with priority call processing.
3. Based on policy:
   - *If no RHP is present*, a RHP may be populated with an ets namespace, with a priority level value of Default (DF).
   - *If an RHP is present with an ets namespace*, the priority level value may be reset to the DF.
4. The packets are priority marked, as defined in clause 8, and transmitted toward the IP backbone, resulting in the packets receiving the highest priority treatment on access to the IP backbone and in the IP backbone.

5.4.3 Core 2 Network to Destination Access

In the following scenarios, it is assumed that validation of the far end sending network has already occurred in the core, and that there is a trust relationship between the core and destination access network.

5.4.3.1 IP Core Network to Wireline Destination Access

Illustrated call/session scenarios can be found in clause 6, flows A & C in Figures 8, 10, 12, and 13. The following actions are taken at the PSTN gateway:

1. The call is provided priority call processing based on the presence of a RPH with an ets namespace.
2. Protocol interworking is performed as shown in Table 2.
3. Current priority call processing continues.

5.4.3.2 IP Core Network to Wireless Destination Access

Illustrated call/session scenarios can be found in clause 6, flows B & D in Figures 8, 10, 12, and 13. The following actions are taken at the PSTN gateway:

1. The call is provided priority call processing based on the presence of an RPH with an ets namespace.
2. Protocol interworking is performed as shown in Table 2.
3. Current priority call processing continues.

5.4.3.3 IP Core Network to IP Destination Access

Illustrated call/session scenarios can be found in clause 6, flowC & D in Figure 11.

The following actions are taken by the core's CCFE and BFE interfacing the destination access (the IP-IP Session Border Control function):

1. The call is provided priority call processing based on the presence of a RPH with an ets namespace. The RPH value(s) are not modified.
2. The packets are priority marked, as defined in clause 8, and transmitted toward the IP Access network, resulting in the packets receiving the highest priority treatment on access to and in the IP access network.

5.4.3.4 TDM Core Network to IP Destination Access

This call/session scenario is not illustrated.

Current call processing occurs at the destination wire line exchange. The following actions are taken at the PSTN Gateway:

1. The call is identified as an ETS call, resulting in priority call processing, by the presence of a CPC value of NS/EP Call.
2. Protocol interworking is performed as shown in Table 1.
3. The packets are priority marked, as defined in clause 8, and transmitted toward the IP Access network, resulting in the packets receiving the highest priority treatment on access to and in the IP access network.

6 CALL/SESSION SCENARIOS

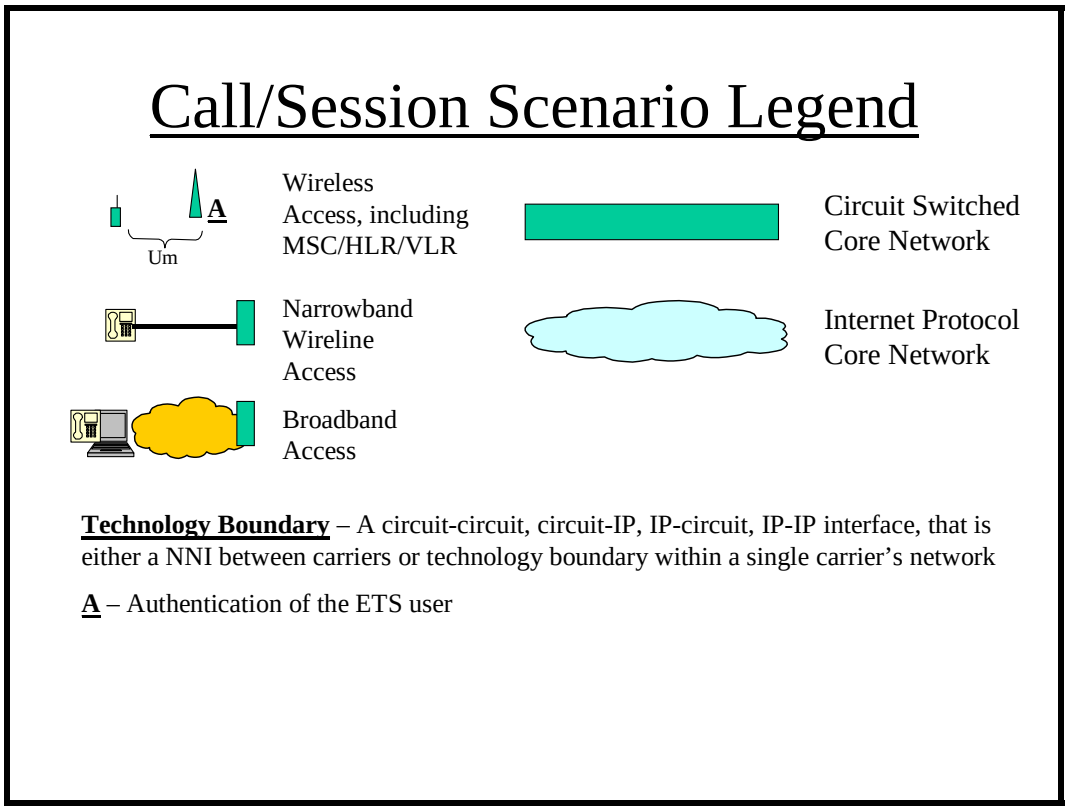

Figure 6 - Call/Session Scenario Legend

Two types of authentication functions are considered in this document.

- ***ETS authentication*** – This type of authentication is invoked when the calling user dials an ETS-DN.
  i. *If the call is authenticated in the TDM domain*, after the call is authenticated:
     - The CPC parameter in the IAM is set to "NS/EP Call".
     - Existing TDM authentication mechanisms do not have the calling user's priority value, so the Precedence parameter is not included in the IAM. If future authentication mechanisms have the calling user's priority value, the Precedence parameter will be included in the IAM.
  ii. *If the call is authenticated in the IP domain*, after the call is authenticated:
     - If the calling user's priority level is not available, only ets.x is created in the RPH, where x is a default priority value based on policy;or
     - If the calling user's priority level is available, both ets.x and wps.y namespaces are created in the RPH, where y is the calling user's priority level and x is based on policy.
- ***WPS authentication*** – This type of authentication is invoked when the calling user dials a WPS-FC+DN.
  i. *If the call is authenticated in the TDM domain*, after the call is authenticated:

- The CPC parameter in the IAM is set to "NS/EP Call".
- If the calling user's priority level is available, the Precedence level (in the Precedence parameter) in the IAM would also be set (precedence level 0 – 4 corresponding to user priorities 1 – 5).

ii. *WPS authentication in the IP domain* (e.g., for UMTS phones) is not addressed in this document.

Successful ETS authentication may result in changing the priority values in the ets or wps namespaces.

The "A" in the figures in this clause represent points of authentication. When placed at the edge, on wireless access, this represents a WPS authentication. For the call/session scenarios in this clause, it is assumed that the calling user's priority level is not available to the ETS authentication function. Therefore, only the ets namespace is created in the RPH after successful authentication; the wps namespace is not created in the RPH.

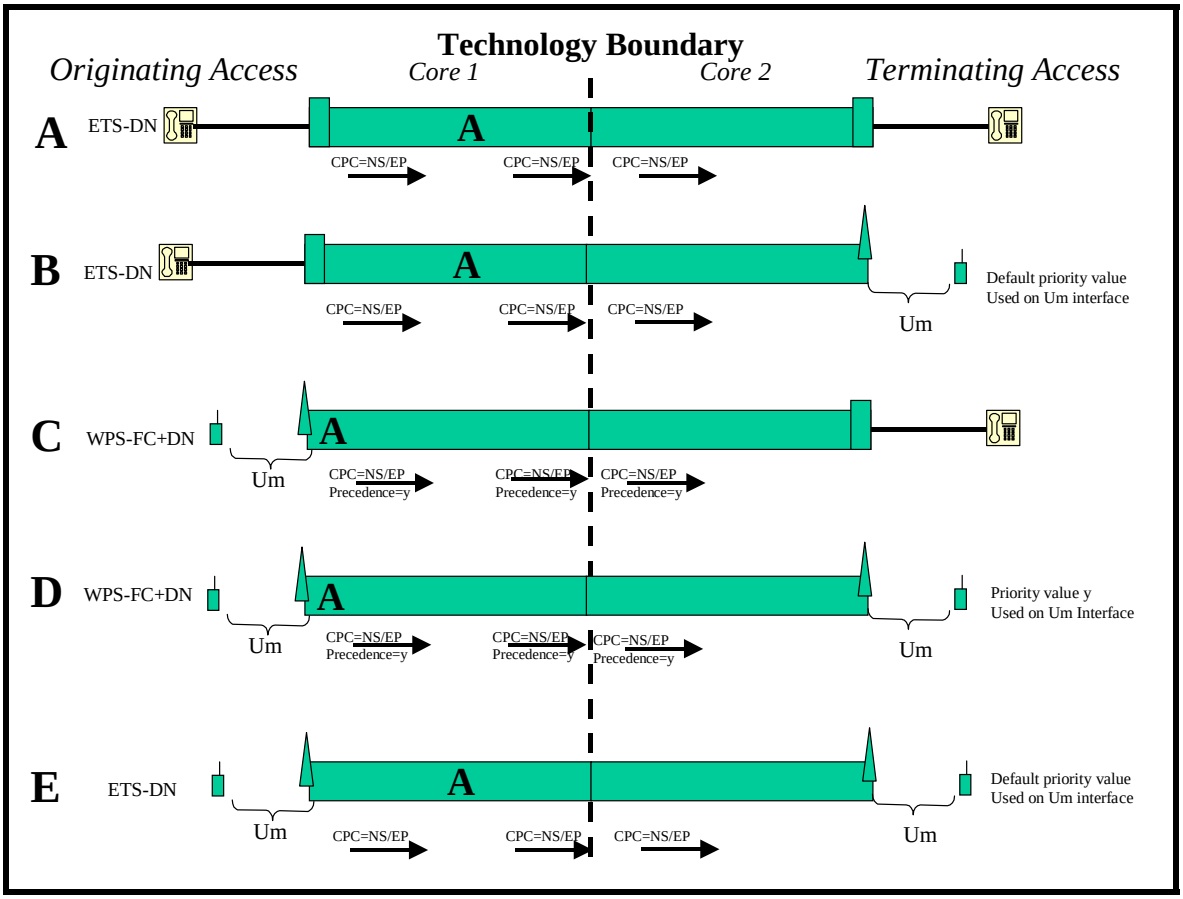

Figure 7 - TDM-to-TDM Network Interconnection

In Figure 7, the WPS calls (**C & D**) are authenticated in the originating wireless network (i.e., the caller's home network) and the ETS calls (**A, B, and E**) are authenticated in the core 1 TDM network.

C & D - A wireless subscriber dials a call as WPS-FC + DN to indicate request for a WPS call. The DN is not an ETS-DN. See Figure 12 (C & D) for call scenarios where a wireless subscriber dials a call as WPS-FC+ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic channel at the originating interface. The IAM includes the CPC coded as "NS/EP Call" and the Precedence parameter corresponding to the WPS priority level of the call.

E - A call that is dialed using an ETS-DN without a WPS-FC is not given priority access to a radio traffic channel at the originating interface. The call is marked as an NS/EP call for priority treatment. The IAM includes the CPC coded as "NS/EP Call", but without the Precedence parameter. The mappings at the NNI as shown in A and B apply for this call scenario.

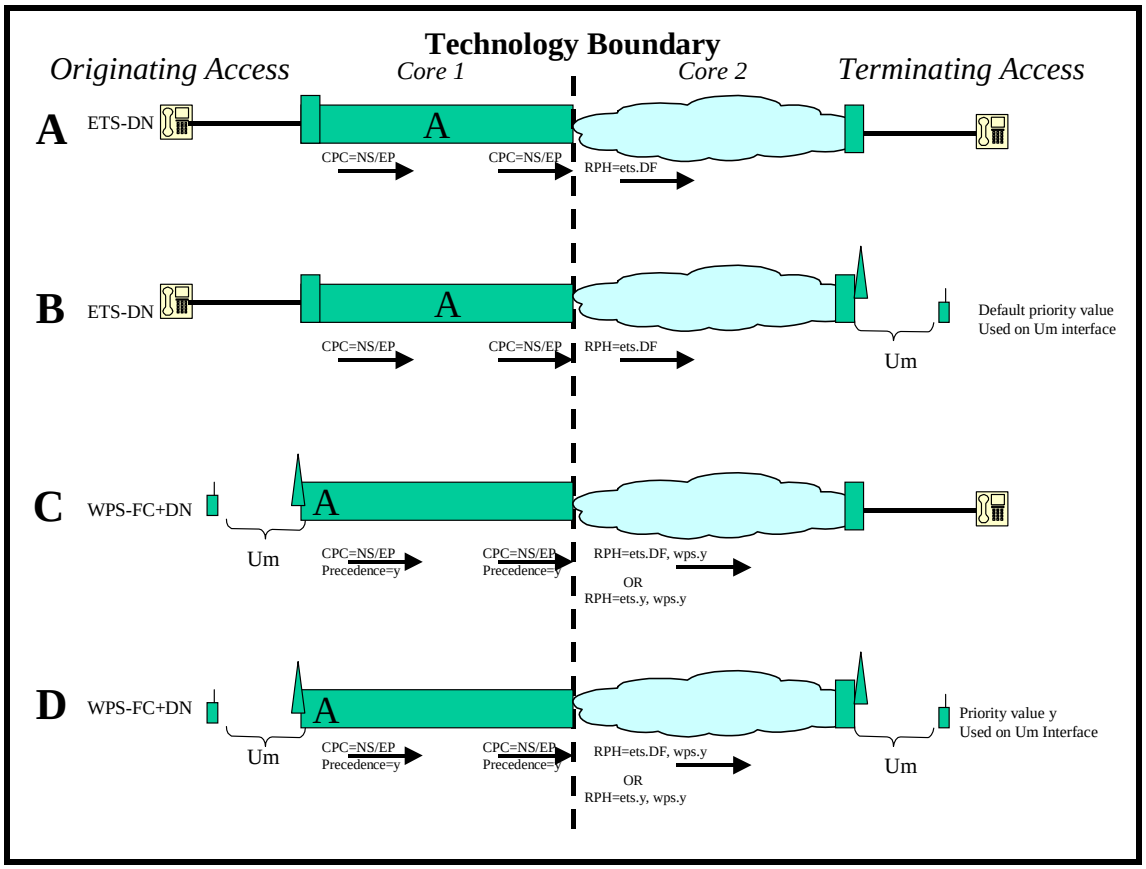

Figure 8 - TDM-to-IP Network Interconnection

In Figure 8, the WPS calls (**C & D**) are authenticated in the originating wireless network and the ETS calls (**A & B**) are authenticated in the core 1 TDM network.

A – Default priority value (DF) in ets.DF is used in the IP core network 2 and is mapped to CPC = "NS/EP Call" in the terminating wireline network.

B – WPS service provider uses a provisioned default priority value at the Um I/F.

C & D - A wireless subscriber dials a call as WPS-FC + DN to indicate request for a WPS call. The DN is not an ETS-DN. See Figure 12 (C & D) for call scenarios where a wireless subscriber dials a call as WPS-FC+ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic channel at the originating interface. The IAM includes the CPC coded as "NS/EP Call" and the Precedence parameter with the WPS priority level of the call. In addition, the priority value from the Precedence parameter is mapped to wps.y in the IP core network 2. Based on policy, ets.DF may carry a provisioned default priority value, or the priority value from the Precedence parameter may be mapped to ets.y.

E (not shown) - A call that is dialed using an ETS-DN without a WPS-FC is not given priority access to a radio traffic channel at the originating interface. The call is authenticated in the TDM core network 1. The call is marked as an NS/EP call for priority treatment within the TDM core. The IAM includes the CPC coded as "NS/EP Call", but without the Precedence parameter. The mappings at the NNI as shown in A and B apply for this call scenario.

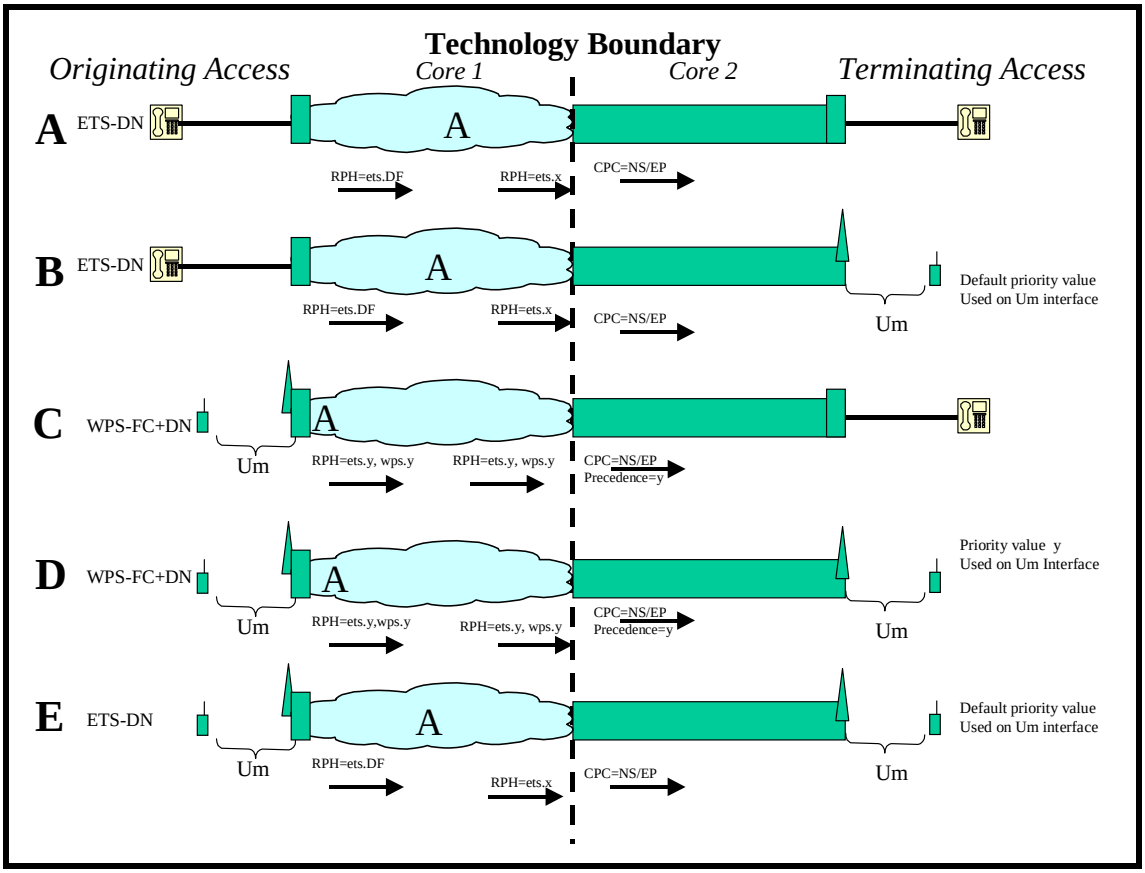

Figure 9 - IP-to-TDM Network Interconnection

In Figure 9, the WPS calls (**C & D**) are authenticated in the originating wireless network and the ETS calls (**A, B, & E**) are authenticated in IP core network 1.

A & B – A wireline call is assigned the default priority value (DF) for the ets namespace at the interface between the originating access network and IP core network 1. The IP network then authenticates the call and, based on policy, changes the priority in the ets.DF to a different value, ets.x.

C & D - A wireless subscriber dials a call as WPS-FC + DN to indicate request for a WPS call. The DN is not an ETS-DN. See Figure 13 (C & D) for call scenarios where a wireless subscriber dials a call as WPS-FC+ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic channel at the originating interface. At the IP gateway from the wireless access network to core network 1, an INVITE message is generated which includes the RPH namespaces ets.y and wps.y indicating the priority level y of the call.

E - A call that is dialed using an ETS-DN without a WPS-FC is not given priority access to a radio traffic channel at the originating interface. The call is marked as an NS/EP call for priority treatment. . The call is assigned the default priority value (DF) for the ets namespace at the point of origination in IP core network 1. The IP network then authenticates the call and, based on policy, changes the priority in the ets.DF to a different value, ets.x. The INVITE message includes ets.x after the call is authenticated, but without the wps namespace. The mappings at the NNI as shown in A and B apply for this call scenario.

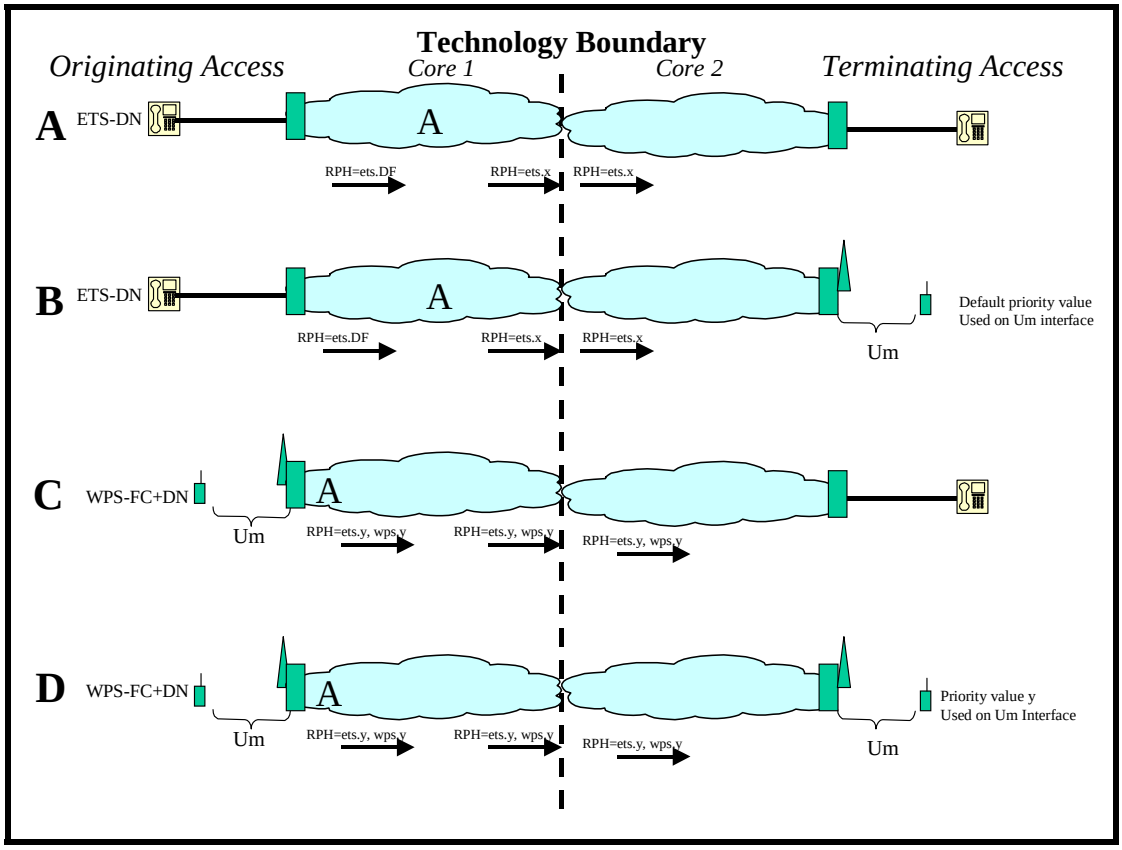

Figure 10 - IP-to-IP Network Interconnection

In Figure 10, the WPS calls (**C & D**) are authenticated in the originating wireless network and the ETS calls (**A & B**) are authenticated in IP core network 1. A trust relationship is assumed to exist between the Core1 and Core 2 networks.

A – If the PSTN gateway between the originating access network and core network 1 supports SIP-I, the SIP messages may contain MIME'd ISUP that may be modified appropriately during ETS authentication in core network 1.

B –The terminating WPS service provider uses a provisioned default priority value at the Um I/F, since no wps namespace is provided.

C & D – A wireless subscriber dials a call as WPS-FC + DN to indicate request for a WPS call. The DN is not an ETS-DN. See Figure 13 (C & D) for call scenarios where a wireless subscriber dials a call as WPS-FC+ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic channel at the originating interface. The INVITE message includes the RPH namespace wps.y indicating the priority level y of the call. In addition, ets.y namespace is also included in the RPH.

E (not shown) - A call that is dialed using an ETS-DN without a WPS-FC is not given priority access to a radio traffic channel at the originating interface. The call is marked as an NS/EP call for priority treatment. The call is assigned the default priority value (DF) for the ets namespace at the point of

origination in IP core network 1. The IP network then authenticates the call and, based on policy, changes the priority in the ets.DF to a different value, ets.x. The INVITE message includes ets.x after the call is authenticated, but without the wps namespace. The mappings at the NNI as shown in A and B apply for this call scenario.

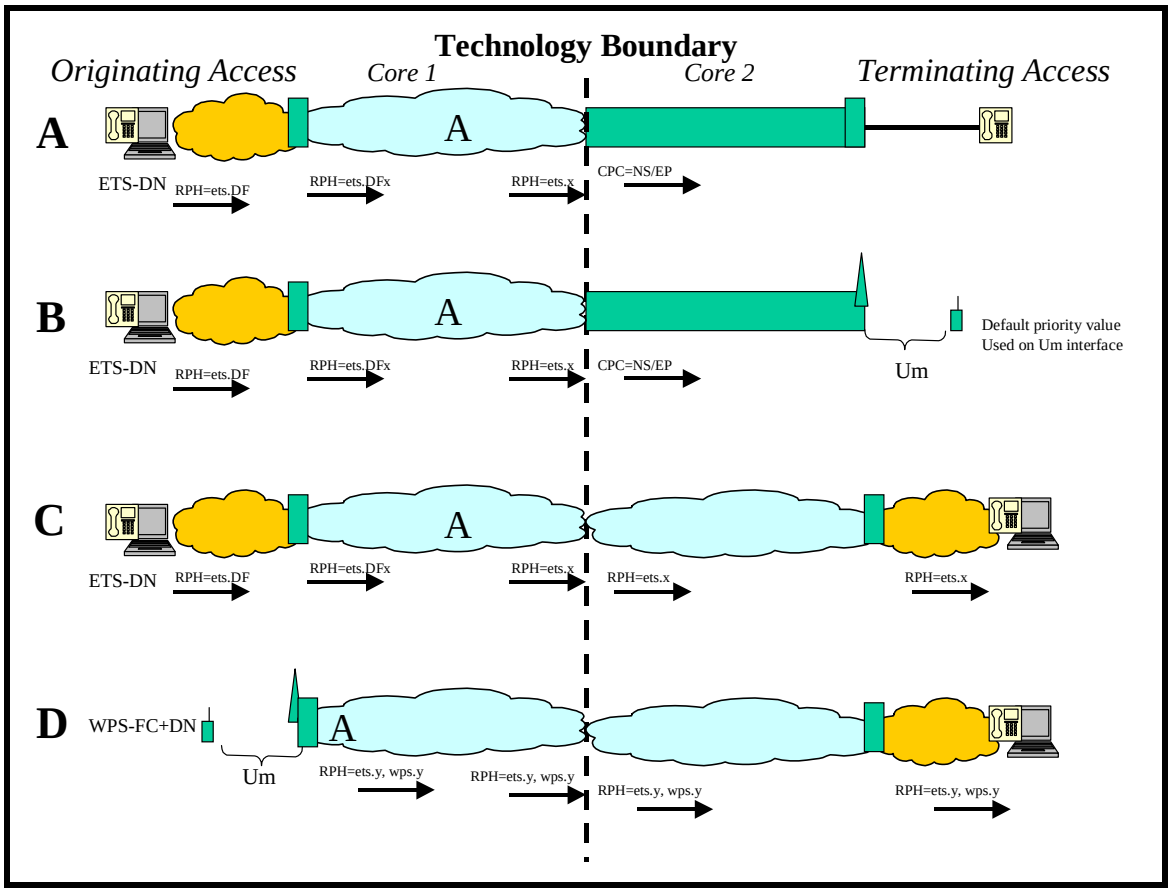

Figure 11 - IP-to-IP Network Interconnection, IP Access Network

In Figure 11, the WPS call (**D**) is authenticated in the originating wireless network and the ETS calls (**A, B & C**) are authenticated in the core 1 IP network.

A, B, & C: Based on policy, the Session Border Control function (CCFE and BFE of core network 1) facing the user may reset the ets priority value (DF) to a provisioned default value (DFx). The IP network then authenticates the call and, based on policy, changes the priority in the ets.DF to a different value, ets.x

D –A wireless subscriber dials a call as WPS-FC + DN to indicate request for a WPS call. The DN is not an ETS-DN. See Figure 13 (C & D) for call scenarios where a wireless subscriber dials a call as WPS-FC+ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic

channel at the originating interface. The INVITE message includes the RPH namespace wps.y indicating the priority level y of the call. In addition, ets.y namespace is also included in the RPH.

E (not shown) - A call that is dialed using an ETS-DN without a WPS-FC is not given priority access to a radio traffic channel at the originating interface. The call is marked as an NS/EP call for priority treatment. The call is assigned the default priority value (DF) for the ets namespace at the point of origination in IP core network 1. The IP network then authenticates the call and, based on policy, changes the priority in the ets.DF to a different value, ets.x. The INVITE message includes ets.x after the call is authenticated, but without the wps namespace. The mappings at the NNI as shown in A and B apply for this call scenario.

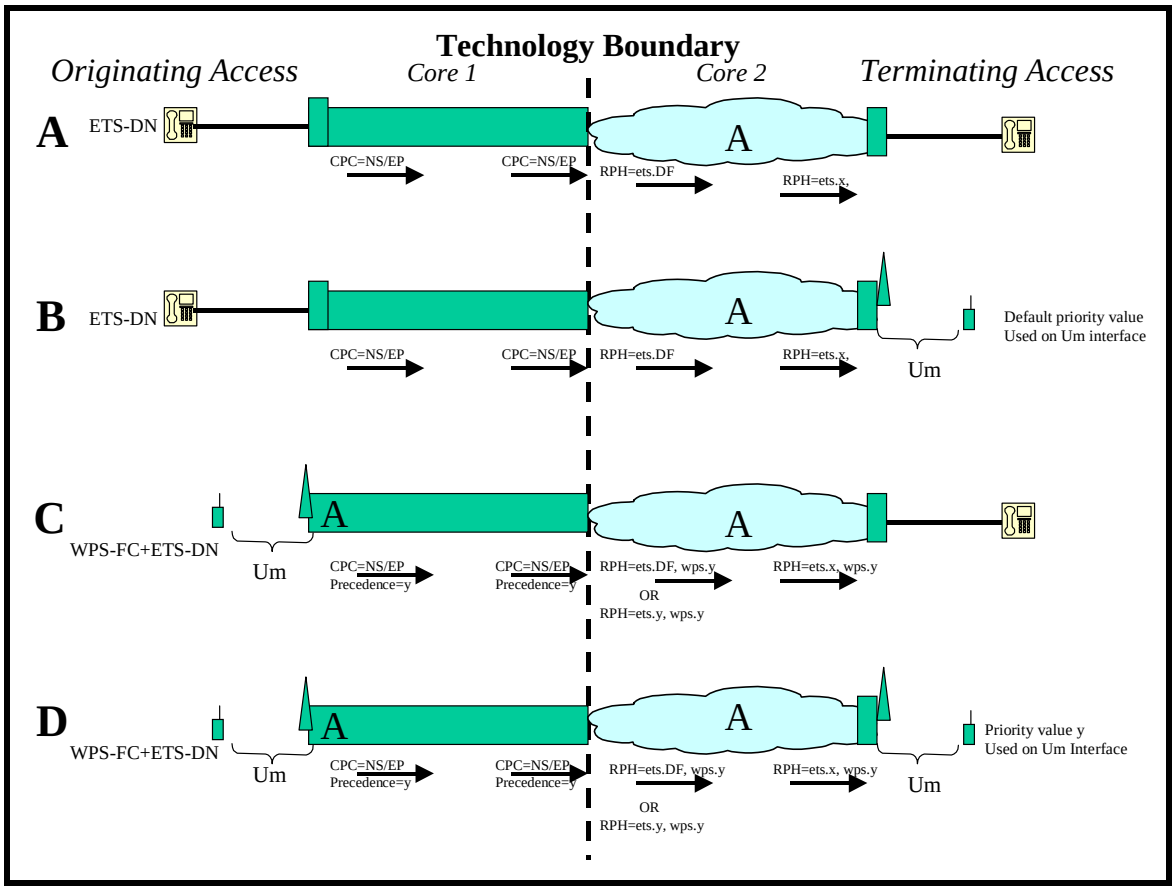

Figure 12 - TDM-IP Interconnection, with Authentication in Core 2

In Figure 12, the WPS calls (**C & D**) are authenticated in the originating wireless network and, because of the ETS-DN, re-authenticated in IP core network 2 . The ETS calls (**A & B**) are authenticated in IP core network 2 .

A & B - A subscriber dials a call using an ETS-DN. Therefore, the call is marked as an NS/EP call for priority treatment. The IAM includes the CPC coded as "NS/EP Call". A Precedence parameter is not included in the IAM. The call is routed, in this case, to an IP-based carrier that is capable of providing

the ETS authentication function. After successful ETS authentication, the call is progressed to the destination. The ETS authentication function may change the pre-authentication priority in the ets.DF to a different post-authentication value, ets.x.

C & D - A wireless subscriber dials a call as "WPS-FC+ DN", where the DN is an ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic channel at the originating interface. The IAM includes the CPC coded as "NS/EP Call" and the Precedence parameter with the WPS priority level of the call. The call is routed, in this case, to an IP-based carrier that is capable of providing the ETS authentication function. Based on policy, core network 2 PSTN-IP Gateway may set the pre-authenticated ets namespace either to a default value (DF) or to y from the Precedence parameter. After authentication, ETS authentication function may change the priority in the ets namespace to a different value, ets.x. After successful ETS authentication, the call is progressed to the destination.

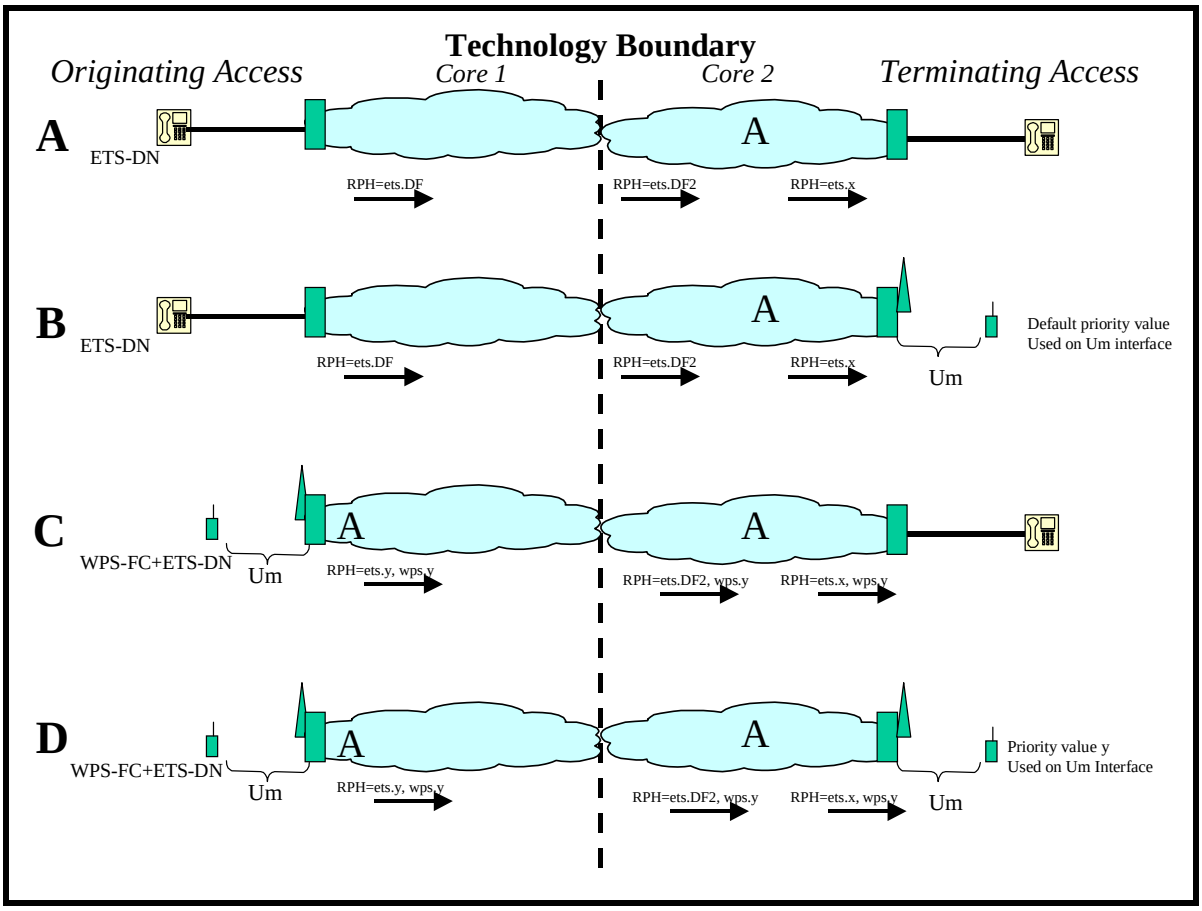

Figure 13 - IP-IP Interconnection, with Authentication in Core

In Figure 13, the WPS calls (**C & D**) are authenticated in the originating wireless network and, because of the ETS-DN, re-authenticated in IP core network 2 . The ETS calls (**A & B**) are authenticated in IP core network 2.

Based on policy, the session border control function (border CCFE and BFE) of core network 2 may reset the received ets priority value (DF or y) to a provisioned default (DF2).

A & B - A subscriber dials a call using an ETS DN. Therefore, the call is marked as an NS/EP call for priority treatment. The INVITE message includes the RPH coded as ets.DF. The call is routed, in this case, to an IP-based carrier that is capable of providing the ETS authentication function. After successful ETS authentication, the call is progressed to the destination. The ETS authentication function may change the pre-authentication priority in the ets.DF2 to a different post-authentication value, ets.x.

C & D - A wireless subscriber dials a call as "WPS-FC+ DN", where the DN is an ETS-DN. If the call is successfully authenticated as a WPS call by the originating service provider, the call is marked as an NS/EP call for priority treatment and is given priority access to a radio traffic channel at the originating interface. The INVITE message includes the RPH namespace wps.y indicating the priority level y of the call. In addition, the ets.y namespace is also included. The call is routed, in this case, to an IP-based carrier that is capable of providing the ETS authentication function. Based on policy, the core network 2 IP-IP Gateway may set the pre-authenticated ets namespace value to DF2. After authentication, the ETS authentication function may change the priority in the ets namespace to a different value, ets.x. After successful ETS authentication, the call is progressed to the destination.

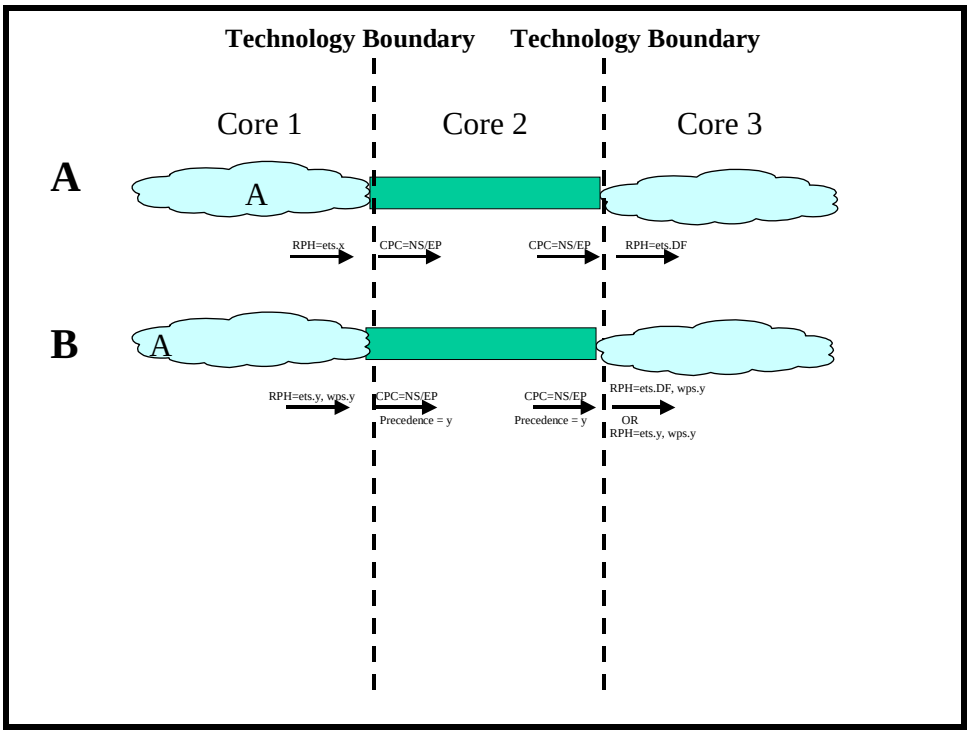

Figure 14 - IP Networks connected via TDM Transit Network

In Figure 14 A, an ETS call is authenticated in core network 1. In Figure 14 B, a WPS call is authenticated in core network 1.

7 SECURITY

7.1 Overview

This clause provides objectives, requirements and guidelines for ETS security. The security requirements are based on the security dimensions defined in ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*, and ITU-T Recommendation X.805.

7.2 Security Objectives and Guidelines

The general objective is to support secure end-to-end ETS communications and protect the availability of ETS.

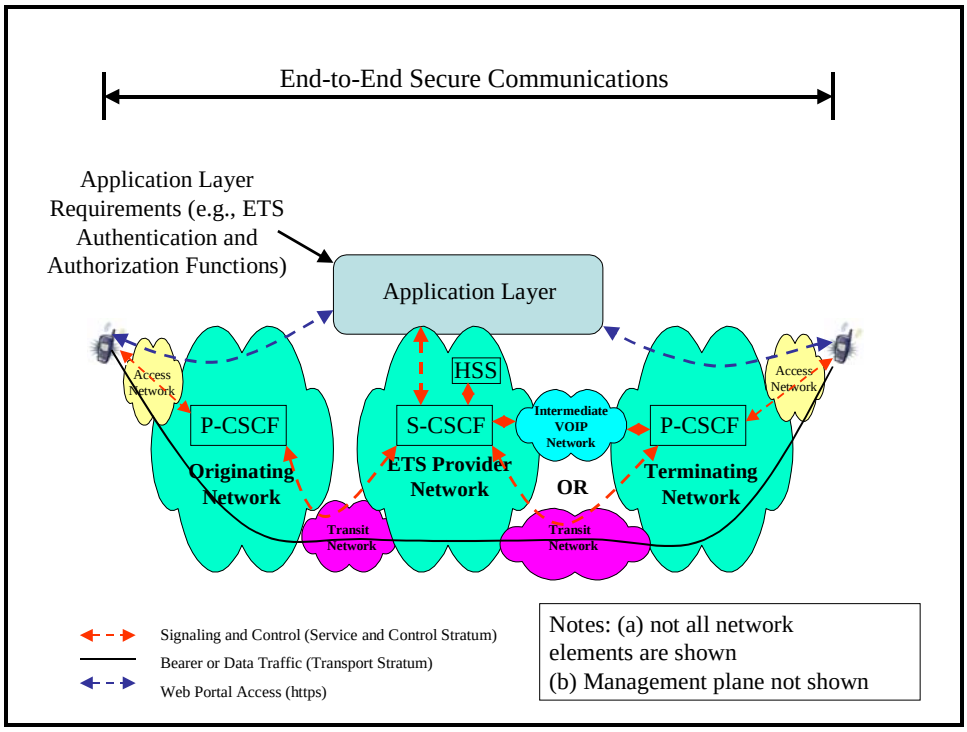

Figure 15 - Example End-to-End ETS Communication

Figure 15 illustrates an example end-to-end ETS communication. The example illustrates that end-to-end communications may traverse multiple network segments and administrative domains (e.g., Access Network, Originating Network, ETS Provider Network, Intermediate Network and Terminating Network). In addition, as described in clause 4, the access and core network segments might be based on different technologies:

- Narrowband wireline (e.g., POTS phone), broadband wireline (e.g., Cable or DSL) and wireless access (e.g., GSM or CDMA).

- IP and circuit-switched (TDM) core networks.

Each network segment will have specific security responsibilities within its administration domain to facilitate end-to-end security and availability of ETS communications.

The following is a minimal set of general guidelines and security planning to protect ETS signalling, bearer and data, and management related data and information (e.g., user profile information):

- Each network administrative domain should establish and enforce security policies and implement mitigation capabilities for ETS within its domain. Specifically, it is recommended that mitigation capabilities and security practices beyond those needed for other services (i.e., mitigation capabilities, practices and policy specific to ETS) should be identified and enforced. For example, these capabilities and practices should be designed to prevent use of ETS services and resources by unauthorized users, and to prevent denial of service and other types of attacks.
- Each network administrative domain should establish methods and procedures for identifying ETS communications, and for identity management and authentication of users and networks across multiple network administration domains. For example, Service Level Agreements (SLAs) should establish security policy for authenticating each domain when handing off and receiving ETS communications.
- Each network administrative domain should establish and enforce security policies to protect ETS management related data and information (e.g., user profile information).

7.3 Security Requirements

7.3.1 General Security Requirements

The following general security requirements shall be supported for ETS:

1. Security capabilities to protect end-to-end ETS communications across multiple network administration domains.
2. Security capabilities to provide identity management and authentication of users and networks across multiple network administration domains. It is highly desirable that the user interact with the ETS service only once and that the security mechanisms pass the user's credentials from administrative domain to administrative domain.
3. Security capabilities to allow ETS authentication/authorization application services from a 3rd party provider.
4. At the NNI with other networks, the network elements supporting the resource priority header must implement SIP over TLS [RFC3546], the sips URI scheme, Digest Authentication [RFC2617] and S/MIME [RFC2633], as appropriate. At the UNI, the network elements supporting the resource priority header should implement SIP over TLS [RFC3546] or IPSec, the sips URI scheme, Digest Authentication [RFC2617] and S/MIME [RFC2633], as appropriate.

7.3.2 Authentication, Authorization, and Access control

The following minimum set of authentication, authorization, and access control capabilities shall be supported for ETS:

- Security capabilities to protect mechanisms used to authenticate and authorize ETS users and devices.
- Security capabilities to protect mechanisms used to bind ETS end user with associated devices.
- Security capabilities to protect mechanisms used to share authentication information (e.g., confirm that a user has been authenticated) across multiple network administrative domains.
- Security capabilities to protect mechanisms used for mutual authentication of user and entities. This includes mechanisms for an ETS user to authenticate the called party or communicating entities (e.g., website, content server, etc).
- Security capabilities to protect mechanisms used to by one network to authentication another network. This includes mechanisms used to authenticate the network handing off an ETS communication (e.g., originating network) and authentication of the network receiving the ETS communication (e.g., intermediate or terminating networks).
- Security capabilities to protect against unauthorized access to ETS information and resources (e.g., user information in authentication servers and management systems).

7.3.3 Confidentiality and Privacy

The following minimum set of confidential capabilities shall be supported:

- Security capabilities to provide confidentiality protection of the ETS signalling and control.
- Security capabilities to provide confidentiality protection of ETS bearer and data traffic (e.g., voice, video, or data).
- Security capabilities to provide confidentiality protection of ETS user and communicating entities identities, and subscription information.
- Security capabilities to provide confidentiality protection of ETS user location.

The following minimum set of privacy capabilities shall be supported:

- Security capabilities to provide privacy protection of ETS information (e.g., information derived from the observation of network activities such as web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network).
- Security capabilities to provide privacy protection against unauthorized observation of ETS usage information (e.g., usage patters such as ETS traffic volume, locations, time, frequency, etc.).

7.3.4 Data Integrity

The following minimum set of data integrity capabilities shall be supported:

- Security mechanisms to provide integrity protection of ETS communications (e.g., protection against unauthorized modification, deletion, creation, or replay). This includes mechanisms to provide notification of information tampering or modification.

- Security mechanisms to provide integrity protection of ETS information (e.g., priority marking, voice, data, and video).
- Security mechanisms to provide integrity protection of ETS specific configuration data (e.g., priority information stored in policy decision functions, user priority level, etc.).

7.3.5 Communication

The following minimum capability shall be supported:

- Security mechanisms to protect ETS communications from an authorized ETS user against intrusions (e.g., mechanisms to prevent interception, hijacking or replay of ETS signalling or bearer/data traffic).

7.3.6 Availability

The following minimum set of capabilities shall be supported:

- Security mechanisms to protect the availability of ETS communications -- e.g., protection of ETS signalling and control, and bearer/data traffic against Denial of Service (DoS) and other forms of attacks.
- Security mechanisms to protect the availability of ETS specific resources and information -- e.g., authentication/authorization databases, priority information stored in policy decision function, and dedicated network resources against Denial of Service (DoS) and other forms of attacks.

8 PACKET PRIORITY MARKING

The presence of an ets namespace in the RPH will result in priority handling which includes priority packet marking resulting in the packets having the highest access to the IP backbone, and highest priority route in the IP backbone.