



21355 Ridgetop Circle
Dulles VA 20166-6503



www.Verisign.com

15 July 2005

Ms. Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

Re: ***Ex Parte* Presentation**

In the Matter of Number Resource Optimization; Qwest Communications Corporation. on Behalf of its IP-Enabled Service Operations, Petition for Limited Waiver of Section 52.15(g)(2)(i) of the Commission's Rules Regarding Numbering Resources, CC Docket No. 99-200

Dear Ms. Dortch:

This is to inform you that Anthony M. Rutkowski (Vice President for Regulatory Affairs) of VeriSign, Inc., by email on 14 July 2005 sent the attached message and document to Sheryl Todd, Mika Savir, Geraldine Matise, Julius Knapp, Guy Benson, Steven Spaeth, and Arthur Lechtman of the Commission's Wireline Competition Bureau, Office of Engineering and Technology, Wireless Telecommunications Bureau, and International Bureau.

The purpose of this information was to convey information concerning ongoing industry activity to support the rapid availability of authenticated VoIP provider and subscriber identification and contact information that presently exists for non-VoIP telephony offerings.

Pursuant to the Commission's rules, this *ex parte* letter together with presentation slides are being filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceedings.

Respectfully submitted,

/s/

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

cc:

Sheryl Todd
Mika Savir
Guy Benson
Steven Spaeth

Julius Knap
Geraldine Matise
Arthur Lechtman

From: Tony Rutkowski [<mailto:trutkowski@verisign.com>]

Sent: Thursday, July 14, 2005 10:21 AM

To: Sheryl Todd

Cc: Mika Savir; Geraldine Matisse; Julius Knapp; Guy Benson; Steven Spaeth; Arthur Lechtman

Subject: docket 99-200 ex parte on requirements for allocation of E.164 numbers for IP telephony

Dear Ms. Todd,

Both on behalf of VeriSign, as well in my capacity as rapporteur on law enforcement assistance and ITU standards groups, I wanted to bring to your attention developments relevant to the current comment pleading cycle in Docket No. 99-200 concerning waiver of Sec. 52.15(g)(2)(i).

Specifically, the issue is - what requirements should be imposed upon ISPs for allotment of E.164 telephone number blocks. VeriSign encourages such availability, but urges that customary requirements under long-standing Commission Rules, as well as domestic and international industry operational arrangements and standards bodies be imposed as a condition of grant. These requirements include the ability to rapidly and authentically determine who is the provider of the VoIP service and who is the subscriber associated with the telephone number - together with the ability to rapidly obtain contact information for the provider and subscriber, but which also meets privacy expectations.

These requirements are critical to meeting the needs of law enforcement support, E-911, critical infrastructure protection, and many other essential needs of the public communications infrastructure. These requirements are also relevant to ongoing proceedings in dockets 04-295 (CALEA), 04-435 (on-board communications), and 05-20 (on-board uplink), among others. See, e.g., "Non-CALEA Operational Capabilities" in the Comments of the Dept. of Justice, et al., in the 04-435 and 05-20 proceedings.

Such authenticated provider and subscriber availability information seems appropriate under long-standing policies established by Computer III, the 1996 Communications Act. The requirements are also highly important in supporting consumer protection features like callerID and ancillary publication services such as raised by the Association of Directory Publishers.

The attached document before the most recent meeting of an ITU-T standards body, describes the ongoing work now occurring. Some of this work specifically related to VoIP implementations in North America is also now occurring in multiple ATIS technical committees, especially TMOC CLDR.

Ultimately, however, the FCC and comparable regulatory, justice, or homeland security agencies in other countries must require ISPs use global industry operational and technical standards for user authentication, provider discovery, and secure availability of their deployed communication identifiers such as telephone numbers and the associated subscriber information.

VeriSign will submit this information as an ex parte submission in the 99-200, 04-295 and 04-435 dockets.

respectfully,

Anthony M. Rutkowski



Question(s): 1, 2, 3, 5, 7, 8, 11/13

Geneva, 25 April-6 May 2005

STUDY GROUP 13 – DELAYED CONTRIBUTION 133**Source:** VeriSign, Inc.**Title:** An NGN Directory Framework Overview - Supporting Critical Operational and Security Requirements

SUMMARY

This contribution describes the current evolving integrated NGN directory framework activity underway in Study Groups 2, 4, 11, 13, and 17 and how it supports critical operational and security capability requirements. The framework includes the ability to discover and securely query authenticated NGN provider and user identification information in highly distributed autonomous databases.

INTRODUCTION

Next Generation Networks worldwide will constitute core public communication network infrastructure. As such, they represent a critical national infrastructure that common to all national infrastructures, have certain design and operations requirements that rely significantly on key common authenticated directory frameworks for providers and users.

In the existing PSTN, all providers worldwide are required to register with a national authority and obtain a unique ITU Carrier Code (ICC) pursuant to ITU-T Rec. M.1400 before the provider can obtain and control network resources using Intelligent Network signalling internets. A related distributed directory capability allows “resolution” of the code into authenticated identification information.¹ Similarly, within most national PSTN Intelligent Network infrastructures, providers then maintain protected directories of authenticated identification information for users – often pursuant to regulatory requirements directed at security, open interfaces, and unbundling requirements.² This common directory architecture constitutes one of the most important foundations for protecting the public infrastructure and meeting an array of operational and public policy requirements. It also enabled commercial services of significant interest to consumers in the marketplace such as CallerID.

¹ See *ITU Carrier Codes*, <<http://www.itu.int/ITU-T/inr/icc/index.html>>

² See, e.g., USA, Telecommunications Act of 1996 (1996 Act), Pub. L. 104-104, 1998 Biennial Regulatory Review – Review of Computer III and ONA Safeguards and Requirements, [diverse rulemakings] in CC Docket No. 98-10.

Contact: Anthony M. Rutkowski
VeriSign Switzerland SA
8 ch. de Blandonnet
Genève 1214

Tel: +1 703 948 4305
Mob: +1 703.362.4668(GSM)
Email: trutkowski@verisign.com

Attention: This is not a publication made available to the public, but an **internal ITU-T Document** intended only for use by the Member States of ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of ITU-T.

These authenticated directory requirements are even more critical for open public IP-Enabled service infrastructures such as NGN. Recognition of this critical need occurred more than twenty years ago with the carefully considered and innovative development of object identifier (OID) namespace within the Open Systems Interconnection (OSI) framework for public internet infrastructure.³ Every object – providers, users, host, and code module had a unique identifier and optional authentication certificate which today. Today, the X.509 certificates serve as an important security tool. Implementation provisions were effected by most Administrations. Even within closed internet infrastructures at the time such as the ARPANET, this need for authenticated directories was underscored by the development of the NICNAME protocol/directory service and a requirement promulgated by the U.S. DOD that any provider or user of internet resources register with the Network Information Center (NIC) and obtain a unique identifier.⁴

COMMON NGN NEEDS AND CAPABILITIES FOR AUTHENTICATED DIRECTORIES

In the NGN environment, the authenticated knowledge of providers and users is critical to just about every requirement relating to security, consumer protection, operations, and competition policy.

National Security and Critical Infrastructure Protection

- network attack mitigation
- public safety emergency and law enforcement assistance
- priority access during or after disasters
- service restoration
- analysis and reporting of network metrics and outages

Consumer Requirements

- consumer emergency calls (E112/E911)
- consumer protection and privacy (Do Not Call; SPAM)
- authenticated caller or sender identification
- disability assistance

Operations Requirements

- service provider coordination
- fraud detection and management
- default service and routing options
- intercarrier compensation
- transaction accounting

Competition Requirements

- number portability
- service interoperability

Similar needs are also incorporated in many if not most of the NGN framework capability set specifications and requirements. This directory information is also critical for nations meeting their obligations under new international treaty instruments for infrastructure protection such as the

³ See, *Information technology - Open systems interconnection - Procedures for the operation of OSI registration authorities: General procedures and top arcs of the ASN.1 object identifier tree*, ITU-T Rec. X.660. See also, James E. White, *A user-friendly naming convention for use in communication networks*, Proc. of the IFIP WG 6.5 working conference on Computer-based message services, Elsevier North-Holland, Inc. New York, NY, USA, 1984.

⁴ See, *NICNAME/WHOIS*, RFC-812, 1 March 1982.

Convention on Cybercrime (Budapest, 2001), COE ITS 185. The challenge revolves around selecting the common global technical and administrative mechanisms for actually implementing the necessary capabilities.

ITU CARRIER CODES AS A GLOBAL NGN PROVIDER IDENTIFIER (NPI)

As noted above, the ITU Carrier Code (ICC) specified in Rec. M.1400 has long existed as a key identifier that allows authenticated national telecommunication service providers to identify themselves in conjunction with OA&M, signalling, and accounting transactions. Some regions like North America refer to this identifier as an Operating Company Number (OCN). In recent standards activity in ITU-T Study Group 4, ETSI TISPAN, and ATIS, this code constitutes part of a unique identifier for every physical object in the NGN telecommunications infrastructure – providing for significantly enhanced inventory management and security.⁵

Three actions are necessary to allow the ICC to serve as the NGN Provider Identifier (NPI). One is for Administrations to require all NGN providers to register and obtain a NPI with appropriate authorities – as is done today for ICCs worldwide in the PSTN, and is not necessarily related to regulatory status. The second is for Study Group 4 to evolve recommendation M.1400 to serve as an effective NPI by making necessary adjustments to the scope, associated identifier fields, and implementation mechanisms. The third is for network-based “rapid resolution” implementations to be established so that authenticated global NPI information can be instantly shared.

The first of these actions is a national matter among regulatory, national security, and industry bodies. In many countries and regions, as NGN, VoIP, and IP-enabled services are already being implemented, the need for a common unique authenticated provider identifier is being faced today.

The second of these actions is already underway under the aegis of the Q1 Rapporteur Group in Study Group 4. The third action was raised in the recent Moscow Study Group 17 meeting, and will be referred to Study Group 4.⁶ A diagrammatic view of the process is depicted in figure 1 below.

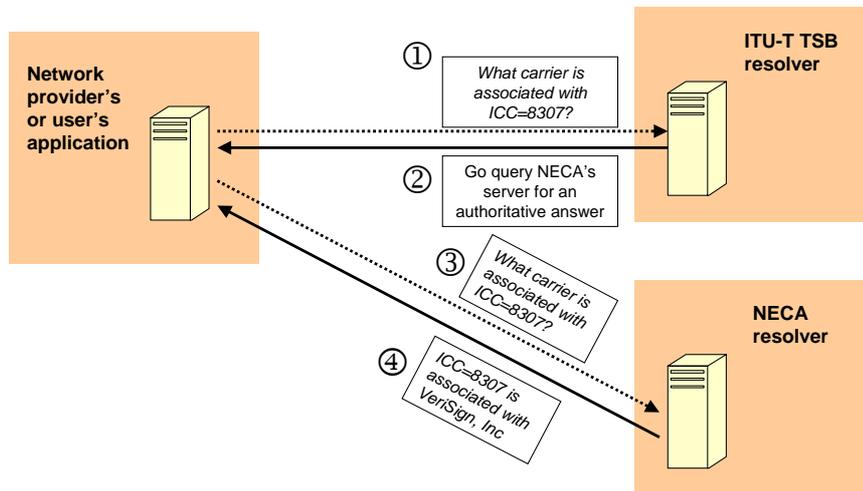


Figure 1. The NGN Provider Identifier Query Process

⁵ See ETSI TISPAN (WG8), *Response to LS from ITU-T SG4 on Equipment Identification*, ITU-T SG4, Doc. TD 17 (GEN), Geneva, 14-25 February 2005; ATIS TCIF 02-004: " Guidelines for data elements included in the Management Information Base," Bar Code/Standard Coding (BCSC) Committee <<http://www.atis.org/BCSC/index.asp>>.

⁶ See *Rapid Resolution of ITU-T Identifiers for NGN*, Doc. COM17-D10, Moscow, 30 March – 8 April 2005.

DISCOVERING AND QUERYING FOR USER IDENTIFIER INFORMATION

The second critical NGN directory capability is related to the provider directory and deals with the ability to discovery and query for authenticated user identifier information. Here also, this capability presently exists and is mandated and maintained worldwide for most public telecommunications infrastructure services. The challenge is to implement an equivalent capability in an NGN environment where the users are much more disparate, nomadic, and global – concurrently employing a multiplicity of service providers with diverse, autonomous directory platforms and implementations.

This challenge was faced several years ago in the Internet Engineering Task Force (IETF), and was the basis for the efforts of the CRISP Working Group and its IRIS protocol platform.⁷ It was this work that was introduced to Study Group 13 at the December 2004 meeting, and became the basis for the E.FIND correspondence group in Study Group 2 at the February 2005 meeting.⁸ The work correspondence group has recently ensued.⁹

The CRISP IRIS platform is now becoming implemented by diverse providers for IP-enabled services. However, it needs further evolution and adoption by the ITU-T and SDOs to serve as a global NGN mechanism. An initial contribution to this effect was submitted to Study Group 17 at its recent Moscow meeting make it apparent that this distributed directory discovery and query should be treated as a directory signalling protocol under the aegis of Study Group 11 rather than a directory protocol.¹⁰ Indeed, Study Group 17 Q2 Rapporteur Group noted that its directory protocol – X.500 – was recently amended to include extensions of significant value to an IRIS like query mechanism.¹¹ A submission to the next Study Group 11 meeting in May will be made by VeriSign.

In order to accomplish the “finding” of NGN user directories enabled by IRIS, the evolution of M.1400 “NGN Provider Identifier” represents a critical enabler. Unless you can discover who the provider is for a user’s services, and how to reach that provider’s authoritative directory of users, you cannot effect a query about a user. The relatively simple inclusion of a directory pointer URI in the set of M.1400 NPI identifier information accomplishes this need. In the query process depicted in figure 1, above, this pointer would be included in part 4 of the query information flow.

INCORPORATING IDENTIFIER INFORMATION SUPPORT INTO NGN CAPABILITY SETS

In addition to accomplishing the above work in other study groups, it remains important for Study Group 13 to consider how identifier information maps into the many requirements and capabilities specified as part of the NGN framework and specifications, and regard the associated support capabilities as a fundamental part of the initial and subsequent specification releases.

⁷ See *Cross Registry Information Service Protocol (crisp)*, <<http://www.ietf.org/html.charters/crisp-charter.html>>.

⁸ See *The NGN Directory Framework – Architecture and Protocols*, Doc. COM 13 – D 65, Study Group 13, Geneva, 7-17 December 2004; *Interworking Framework Among NGN Directories – Operational Requirements*, Doc. COM 2 – D 12, Study Group 2, Geneva, 16-24 February 2005; Project 14, Item 9, *Progress report for Question 1/2*, Doc. TD50 Rev 2 (WP 1/2), Sec. 3.21, Q1/2 (services).

⁹ See <tsg2find@ties.itu.ch>

¹⁰ See *NGN Directory Interworking Framework*, Doc. COM 17 – D 15, Study Group 17, Moscow, 30 March - 8 April 2005.

See *Q2/17 Meeting Report*, Doc. TD 1034 Rev2, Study Group 17, Moscow, 30 March - 8 April 2005.