

4 April 2008

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* Presentations**

In the Matter of: *Free Press, et al., Petitions for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management" and Vuze, Inc. to Establish Rules Governing Network Management Practices by Broadband Network Operators Broadband Industry Practices*, WC Docket No. 07-52

In the Matter of: *Developing a Unified Intercarrier Compensation Regime*, CC Docket No. 01-92

Dear Ms. Dortch:

This is to inform you that Anthony M. Rutkowski, VP of Regulatory Affairs and Standards at VeriSign Inc, met at Commission headquarters on 3 April 2008 with Scott Bergmann (*Senior Legal Advisor, Legal Advisor for Wireline Issues to Commissioner Jonathan S. Adelstein*), and on 4 April individually with Scott M. Deutchman (*Competition and Universal Service Legal Advisor to Commissioner Michael J. Copps*), Cris Moore (*Legal Advisor to Commissioner Deborah Taylor Tate*), John W. Hunter (*Special Counsel, Wireline to Commissioner Robert M. McDowell*), as well as with Carrie-Lee Early and Richard Nunno of the International Bureau.

The purpose of these meetings was to provide an overview of current **Trusted Service Provider Identity (T-SPID)** developments related to the subject proceedings, including potential related actions of the Commission to implement T-SPID. The attached slides formed the basis of dialogue, and convey the substance of what was discussed. In response to staff questions, Mr. Rutkowski pointed out that the Commission presently manages a number of provider identifiers that would be unified with T-SPID, and noted that a core T-SPID document was before an upcoming meeting of the intergovernmental-industry body, ITU-T, at <ftp://ties.itu.int/tsg17/sg17/documents/c/T05-SG17-C-0286!!MSW-E.doc>

VeriSign looks forward to continued collaboration with the Commission in considering matters relating to Trusted Service Provider Identity generally and in the context of the subject proceedings.

Pursuant to the Commission's rules, this *ex parte* letter, together with presentation notes, 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  
21355 Ridgetop Circle  
Dulles VA 20166  
tel: +1 703.948.4305  
<mailto:trutkowski@verisign.com>

cc: Scott Bergmann  
Scott M. Deutchman  
Cris Moore

John W. Hunter  
Carrie-Lee Early  
Richard Nunno

Dockets 07-52, 01-92  
Ex Parte Presentation

Before the  
Federal Communications Commission  
Washington DC

# **A Network Management Essential: Commission implementation of Trusted Service Provider Identity**

Anthony M Rutkowski  
Vice President for Regulatory Affairs and  
Standards  
Dulles VA USA  
tel: +1 703.948.4305  
mailto:trutkowski@verisign.com

# An essential, simple network management step

- The Commission should implement an infrastructure capability for service provider trust
  - Irrespective of other action taken in response to the Vuze Petition on Internet management...
  - A trusted ability to know service provider identity in today's complex network environment was implied by the positions of nearly all commenting parties in Docket 07-52 and is a necessary predicate to minimizing "phantom traffic" in the Docket 01-92
- Different forms of registrations are already required by the Commission, other agencies, and industry bodies for many kinds of service providers...however
  - Everyone has a different registration scheme, sometimes several
  - None are compatible or interoperable
  - None enable automatic instantaneous network lookups that enable trust assessments when dealing with a provider
- A simple, core network management step
  - enable automatic instantaneous network lookups that enable trust assessments when dealing with a provider

# Everyone wins (except bad actors)

- Interested parties
  - Other providers (transport, content, application)
  - Consumers
  - Government
  
- Common needs
  - Reliable network and services operation (public, private, and governmental)
  - Business transactions and settlements
  - Consumer protection
  - Cybersecurity and Critical Infrastructure Protection
  - Regulatory compliance and law enforcement
  - Homeland security, including emergency telecoms
  - DOD Global Information Grid requirement

# The need is now

- Threats and Abuses Abound
  - Cybersecurity threats, identity theft, attacks on government networks, SPAM, large scale fraud, loss of emergency network capabilities, cyberstalking, CallerID spoofing, phantom traffic, etc.
  
- How We Got Here
  - Historically trust was provided by closed, fixed networks with Title II regulation
  - Open public networks (e.g., Internet), wireless, globalization, smart terminal devices, application providers, and shift away from Title II regulation occurred without a necessary common trust infrastructure
  
- Action Needed Now
  - The abuses are now exponential; and the consequences will get much worse without an effective remedy
  - The threats are global, and governments worldwide want solutions

# Initial action is already underway

- Trusted SPID recently emerged in global intergovernmental-Industry forums for network security cooperation
  - Concentrated in new work of the ITU and ISO
  - Follows a year of work among scores of different Identity Management organizations, including DOD Global Information Grid specifications
  - Initial Trusted SPID standards and demonstration slated for 2008
  
- Simple, decentralized, open, low-cost, regulatory-minimal
  - Assign a unique SPID Identifier to every provider worldwide through trusted registries that support a common platform that allows instant discovery and lookup of identity resources associated with the provider.
    - Enables other providers and users to make trust decisions when relying on a provider's identity and assertions
    - Fosters a means for trust resource services innovation and development
    - Builds on existing, distributed, robust, open "resolver" platforms (no centralized databases)
    - Technology neutral

# Necessary steps

- Implementing a universal global means for trusted provider identity
  - Establishes an easily achievable infrastructure solution
  - Enhances transaction efficiencies for all parties
  - Enhances privacy and other consumer needs
- Global government-industry cooperative action are needed
- Government involvement is key
  - Marketplace/industry, technology, R&D, or national action alone, will NOT solve the network management identity challenges
  - The technology exists - leadership, commitment, cooperation, and action are required
  - Regulatory, contract, tort, and copyright law plus procurements and the marketplace worldwide will drive implementation
- A registration-based trust infrastructure is not regulation
- Also responsive to problems relating to telephone and SMS Phantom Traffic and fraudulent CallerID, ref. CC Docket 01-92
- The 07-52 and 01-92 dockets provide an opportunity to establish an essential Trusted Service Provider Identity capability and responsive to the needs of all parties