

**Ofcom
Office of Communications**

**Next Generation Networks:
Further consultation**

COMMENTS OF VERISIGN, INC

Including VeriSign UK Limited

12 August 2005

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
USA
tel: +1 703.948.4305
<mailto:trutkowski@verisign.com>

1. INTRODUCTION

These comments are responsive to Ofcom's further consultation document of 30 June 2005, including the seven Annexes.¹ Of special interest is Annex 7 dealing with Network Intelligence.

For more than a decade, VeriSign has provided an array of large-scale, ultra-high availability, trusted intelligent infrastructures that enables signalling, security, identity management, directory, financial transaction, and fraud management capabilities for just about any kind of network based business and consumer services – whether it be Internet, Web, Internet access, traditional voice telephony, VoIP, multimedia, next generation, or sales. VeriSign operates through various divisions that have offices and staff in the UK and worldwide. In these various capacities, it participates in scores of different forums, working collaboratively with both industry and government.

The emergence of open IP-enabled networks and applications inherently requires much greater network intelligence than for legacy PSTN infrastructure that severely restricted the availability of network resources to users and other network providers, that supported very limited services, and that was bereft of any nomadic capabilities except for commercial cellular users. Conversely, IP-enabled networks of always-on, highly nomadic human and object users using a constantly changing array of access mechanisms require significant, diverse levels of trusted and robust network intelligence to properly support the public infrastructure for communications, commerce, and content. It is this underlying intelligent infrastructure which

¹ See Ofcom Office of Communications, *Next Generation Networks; Further consultation*, 30 June 2005 (hereinafter referred to as “*NGN Further Consultation*”); *ibid.* Annexes (hereinafter referred to as “*NGN Further Consultation Annexes*”).

collectively constitutes VeriSign's principal products, and which are core components of a Next Generation Network environment, and the VeriSign's focus in this consultation response.

2. General Comments

The consultative is impressive in its scope of treatment of NGN developments, its analysis, and depth of detail on key issues. However, it is worth reflecting on a number of important dimensions of NGN national policy that definitely deserve significant treatment. These dimensions include the concern already raised by BT – namely that given the relatively inchoate state of NGN developments, whether the further consultation is attempting to be excessively detailed and determinative too quickly. In this dive into some details, VeriSign suggests that what is being missed are a number of broad critical considerations that are entirely omitted from the consultation and beg for substantive treatment as part of any NGN regulatory regime.

2.1 Critical Infrastructure Protection and Law Enforcement Support

Public IP-enabled Next Generation Networks create very significant challenges for government communities responsible for supporting the requirements to protect the national infrastructure and law enforcement's investigative and forensic needs. There are large-scale initiatives toward this end throughout the world and in the United Kingdom. Furthermore, as highlighted by recent terrorist events, communications forensics capabilities are vitally important to the safety of the nation.

However, these needs are not even recognized, much less substantively treated in the consultative proceeding – even though infrastructure protection and law enforcement support are threaded through nearly every subject treated, especially Intelligent Infrastructure. If the proper and necessary national administrative security mechanisms, as well as the required capabilities put into place by operators –

especially authentication – NGNs become highly vulnerable and a threat to the national and global infrastructure upon which the government, business and the public vitally depend.

These infrastructure protection and law enforcement support considerations are also very relevant to effecting a level competitive playing field. All providers must be subject to the same requirements, lest some become either become subject to an unfair burden or become the “weakest links” exposing the entire infrastructure to vulnerabilities and the nation to terrorist and criminal acts.

The most essential of NGN requirements revolves around the ability for all parties – including government authorities – to know the authenticated identity of all NGN service providers and users, including their communication identifiers, and be able to securely obtain contact details as necessary. No entity other than government authority can effectively impose and enforce such uniform capability requirements, and it should be done in concert with other government authorities worldwide. These trusted identification requirements are also essential to a host of other NGN government needs, consumer protection, effective competition, and operational capabilities. The standards and operational details should in large measure be left to industry, but the requirements must exist from the outset – in common with all public infrastructures where providers and users control the use of resources.

2.2 Importance of NGN Network Intelligence and Competition Requirements

Sec. 1.15, *et seq.*, and Question 4 in the NGN Further Consultative discuss unbundled access to network intelligence. In addition, Annex G contains a relatively thorough treatment of important NGN network intelligence capabilities. However, the Further Consultation stops rather abruptly with the statement “[t]here are also questions about how network intelligence information would be exchanged between

competing providers...[h]owever, it is less clear that there is potential for competition concerns relating to this, and we do not consider this aspect in detail here.”²

VeriSign submits that this issue is among the most important in the entire ensemble of NGN issues, and its effective treatment and associated regulatory framework is critically important not only to NGN competition, but to meeting an array of other important NGN requirements associated with national security and consumer protection. This importance is underscored by the fundamental large-scale shift in competition paradigms in an NGN world from facilities based competition to intelligent infrastructure and applications-based competition. It involves more than just unbundling. It involves an ensemble of requirements that history over the past twenty years has proven essential.

In the 1980s, the telecommunications community worldwide undertook an effort analogous to present NGN developments, and proceeded to develop standards and frameworks for a next generation “internetworking” intelligent network architecture.³ However, the marketplace and associated capabilities largely emerged only in the USA because their Federal Communications Commission established an industry-driven regulatory Open Network Architecture framework that consisted of three pillars: open interfaces, access to unbundled intelligent infrastructure network elements, and reciprocal access to authenticated directory information.⁴ There is every reason to believe that these requirements will be even more significant in an NGN environment because of the far larger ensemble of both facilities-based and non-

² Para. G.4, *NGN Further Consultation Annexes*.

³ See, e.g., ITU-T Rec. Q.1200, General series Intelligent Network Recommendation structure (1997-09), *et. seq.*

⁴ See *Report and Order in the Matter of Amendment of Sections 64.702 of the Commission’s Rules and Regulations (Third Computer Inquiry); and Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Thereof; Communications Protocols under Section 64.702 of the Commission’s Rules and Regulations*, in CC Docket No. 85-229, 16 June 1986.

facilities-based providers, the more open network nomadic access mechanisms, and the richer array of applications today using IP-enabled platforms.

The NGN Further Consultation Annex G does treat the subject of NGN directories.⁵ However, does so in a very narrow technical fashion that ignores available open industry distributed directory access and sharing mechanisms, as well as the very significant competition, national security, and public policy considerations.⁶ The notion that a single central user directory database is needed or otherwise appropriate for any purpose, including number portability, is a proposition that is decidedly wrong-headed in an NGN environment. The interworking of distributed directories is the only feasible means of getting trusted current information in a highly dynamic, distributed NGN IP-enabled NGN environment. It is also more robust – eliminating a single point failure potential, and enables competitive solutions.

VeriSign is a global leader in providing most of the capabilities discussed within the Network Intelligence section of Annex G, and expresses through this consultation, its desire to participate competitively in the UK market for most of these NGN services. In that connection, VeriSign urges Ofcom to take appropriate steps to assure open competitive opportunities for these services, including the important three-fold requirements for secure open interfaces, unbundled intelligent network element availability for dominant providers, and reciprocal access to directories associated with users and related presence, authentication, location, and security information.

⁵ See Directory, paras. G.21-G.24, *NGN Further Consultation Annexes* at 27.

⁶ See, e.g., *Interworking Framework Among NGN Directories – Operational Requirements*, ITU-T Doc. COM 2 – D 12 (Feb 2005); *An NGN Directory Framework Overview - Supporting Critical Operational and Security Requirements*, ITU-T Doc. COM 13 – D 133 (May 2005); ETSI TC LI, *The E.FIND Framework and LI*, Doc. TC LI (2005) 08ltd017 (Feb 2005); ETSI TC LI, *NGN Identifier Information Discovery for Lawful Access*, Doc. TC LI (2005) 09ltd026 (Jun 2005).

2.3 International collaboration

Considering the inherently global nature of NGN developments, and that widespread collaboration is occurring on these same issues in European Union forums, in the International Telecommunication Union, and other countries, it is not clear why none of this activity is referenced or treated in the consultation. In addition, the Convention on Cybercrime – of which the UK is a signatory – has recently come into force and bears upon NGN policies.⁷

The almost borderless transparency of IP-enabled Next Generation Networks also inherently raises a panoply of international issues and necessitates continuing collaboration with the regulatory, justice, and infrastructure protection authorities in multiple jurisdictions.⁸ NGNs will necessitate substantially greater real-time operational collaboration than for legacy networks. None of these matters are treated either substantively or as part of an ongoing collaborative process going forward. Some of the recent developments in this area provide an ample basis for further treatment.⁹

3. Discussion Points

Question 1. Do you agree with Ofcom's proposed approach for the charges of narrowband voice SMP products provided over next generation interconnects?

VeriSign has no comment.

⁷ See *Convention on Cybercrime* (Budapest, Nov 2001), Council of Europe Treaty Series 185.

⁸ See, e.g., European Commission, *Open Workshop Identifying Policy and Regulatory Issues*, Next Generation Networks, Brussels, 22 Jun 2005; *ITU Thematic Meeting on Cybersecurity*, Geneva, Jun 2005.

⁹ *Ibid.*

Question 2. Do you agree with the overall approach that there needs to be continuity for existing SMP products, but that it would not appropriate to continue them indefinitely?

Question 3. Do you agree with the general criteria Ofcom has proposed for the withdrawal of legacy SMP products after an interim period?

VeriSign strongly supports the continuity of existing public telecommunication service products as long as there is a significant demand in the marketplace. However, in the absence of adverse public policy or competitive consequences, these seem like matters appropriately decided by BT based on commercial considerations.

Some of the attendant discussion, however, conveys the impression that “NGN” represents a singular, definitive, unified path for the future of all communications. The more likely and desirable conceptualization and model is one of “NGNs” that consist of a diverse ensemble of both public and private network and services capable of interoperating with each other and supporting legacy and non-NGN capable capability sets indefinitely.

Question 4. Which network intelligence capabilities are likely to be associated with the underlying network where BT has SMP and cannot be independently provided by alternative providers, and why?

See the extensive treatment of this subject in sect. 2.2, above. VeriSign believes this question is inappropriately constructed. The issue revolves less around whether someone else can provide BT network intelligence capabilities, but rather whether other provider can gain access to those capabilities, and whether everyone participates on a level intelligent infrastructure playing field based on open interfaces, unbundled signalling network elements, and reciprocal access to directory information including ancillary information such as presence, availability, authentication, and location.

Question 5. What are your views of the practical implications of applying Equivalence of Input to NGNs (eg in relation to MSAN interconnection, end-to-end quality of service, and depth of network hooks)?

VeriSign has no comment.

Question 6. Do you agree with the issues Ofcom has identified that need to be addressed by all communication providers as they move to NGNs and what others are there?

As discussed in Section 2, above, as well as the conclusion, below, many critical issues have not been treated in this consultation, and require full consideration going forward.

Question 7. Do you agree with the policy principles Ofcom has identified for consumer protection during the move to NGNs?

The enunciated policy principles seem rather narrow and substantially undeveloped. Consumers have an array of vital safety, fraud protection, intrusion mitigation, privacy, and other needs that will be much more significant and difficult to address on NGN platforms. The subject of consumer protection deserves fuller treatment.

Question 8. Do you agree with the overall processes for developing 21CN obligatory products?

This process needs further development in light of the issues raised in section 2, above.

Question 9. Do you believe that there is a need to co-ordinate and steer cross industry NGN issues which is not met by existing bodies and process?

VeriSign concurs with this conclusion.

Question 10. Do you agree that there is a need to co-ordinate the planning and implementation of NGNs on an industry wide basis?

VeriSign concurs with this conclusion.

Question 11. Is there a need for a process to address the wider consumer protection issues arising from the move to NGNs?

In light of the response to Question 7, above, there is such a need.

Question 12. Has Ofcom identified all the correct industry processes that will be needed to deal with move to NGNs?

The processes need further consideration in light of the comments in section 2, above.

Question 13. Do you agree that it appropriate for Consult 21 to continue to take responsibility for developing detail of SMP product migration and development of new products?

VeriSign has no comment.

Question 14. Do you agree that Consult 21 combined with bi-lateral commercial negotiation and backed-up by Ofcom dispute resolution is the best approach to the agreeing the commercial aspects of new and migrated products?

VeriSign has no comment.

Question 15. Do agree that NICC should continue to be responsible for standardisation of NGN interconnect, but needs to be re-constituted as an independent industry owned body?

VeriSign has no comment.

Question 16. What are your views on the establishment of a new multi-lateral industry group to address NGN issues, its terms of reference and governance arrangements?

This action seems useful.

Question 17. What are your views on the establishment of a NGN operational dispute adjudicator, its terms of reference and governance arrangements?

Question 18. Would your organisation be prepared to sign-up to such an adjudication scheme and abide by the adjudicator's decisions?

This action seems useful. VeriSign demurs on any commitments at this time.

4. Conclusion

Ofcom states that the objective of the consultation is “to establish a clear policy framework and ensure that robust industry-led processes are in place to take forward the issues.”¹⁰ Whilst good – even pioneering – progress has been made in this consultative proceeding toward that objective, it seems clear that further consultative activity and deliberation is necessary. This seems especially the case for some of the really critical components for an NGN policy framework described in these comments. In addition, such further deliberations would allow further collaboration with other relevant UK government agencies and policy making counterparts elsewhere.

¹⁰ Para 1.3, *NGN Further Consultation* at 1.