Workshop report template

1. Title
New Technical and Policy Challenges in DNS Root Zone Management

2. Organizers and Panelists
<u>Organizers</u>: Internet Governance Project, Third World Network

<u>Moderator</u>:
Milton Mueller, Syracuse University School of Information Studies and IGP

<u>Panelists</u>:
Thierry Moreau, Connotech, Canada
Riaz Tayob, Third World Network, South Africa
Marilyn Cade, Consultant, USA
Brian Cute, VeriSign, USA
Frederico Neves, Director of Services and Technology, Registro.br, Brasil
Lars-Johan Liman, Autonomica.se (root server operator), Sweden

3. Discussion
The panelists and audience vigorously aired conflicting views on the political, economic and technical issues raised by management of the DNS root zone file. The panelists and audience all seemed to agree that this topic was "the elephant in the room" and that it was time to discuss it openly. There agreement that the session succeeded in reducing the size of the elephant, but some felt that the issue of DNSSEC keys (see below) may added a new elephant.

On the issue of unilateral control by the U.S. government, some felt that the situation was tolerable as long as the arrangements are stable and the root server operators have one clear authoritative source for the root zone file. They also mentioned the risk of losing coordination in a move to a new arrangement, stressing the need for caution. Those willing to tolerate the status quo did acknowledge, however, the possibility of an arbitrary unilateral action that could strain or break down global coordination. The discussion explored the potential benefits and dangers of a move to multi-lateral or internationalized root zone file management. One panelist offered a detailed proposal to internationalize root oversight and argued that it would remove a huge distraction from the ICANN regime and improve stability. The proposal was divided into 4 parts and covered 1. Articulation of the limited purpose of governmental oversight and identification of categories of root zone file changes that pose no stability or security threats and can be automated; 2. creation of a multi-lateral governmental advisory committee within the ICANN regime to review root zone file changes; 3. calling up the U.S. and other governments to respect the concept of private sector leadership; 4. Making ICANN more transparent and accountable. Only section 2 of this proposal created major controversies. A panelist argued that whatever new arrangements are adopted must give excluded developing countries a voice in the regime; others complained that section 2 would bring destructive intergovernmental conflict into a domain that should be governed by commercial and technical criteria. A panelist noted progress in ICANN's ccNSO toward automation of routine changes in the root zone file.
DNSSEC is a new IETF standard that uses public-key cryptographic signatures to ensure the integrity and authenticity of DNS data. A key policy issue with DNSSEC is whether or not the root zone file is signed. The decision to sign or not (and the operational processes and security policies chosen) shifts the burden of adoption among the various stakeholders. It is possible to

implement DNSSEC without signing the root, but this creates "islands of trust" in specific TLDs and poses key management and rollover problems for those implementing DNSSEC at levels lower than the root, including registries, who lack strong economic incentives to adopt it on their own. A more fundamental discussion concerned the possibility of alternative roots or coordination configurations that do not rely on a single centralized point at the top of a hierarchy. Most business and technical stakeholders expressed their strong support for the current approach (a single, centralized root); a panelist viewed alternative roots as legitimate political response to the problem of unilateral U.S. control; a member of the audience mentioned coordination mechanisms in the telephone industry that do not require a single operationalized root.

The main outcome of the workshop was to identify more focused areas for further discussion and consensus, which are outlined below under number 5.

4. Inventory of events and actors related to the issue under discussion

Actors
U.S. Department of Commerce, NTIA and NTIS
VeriSign Corp.
ICANN and its IANA function
IETF; All root server operators; All TLD registries; Domain name registrars

Events
New IANA contract; New Registry contracts being considered by ICANN; VeriSign-ICANN-DoC Settlement

5. Possible follow-up
A future workshop or workshops, e.g. at Rio, should take up the following issues identified here:
- If DNSSEC is implemented in the current system, who would sign the root zone and who would hold the keys? What other procedural changes in root zone file management should be considered?
- Should DNSSEC implementation be required in ICANN contracts?
- What aspects of root zone file management can be easily automated and which need to be reviewed?
- What accountability and transparency improvements in ICANN would make it possible to complete the transition to full autonomy?