IPv6 Task Force Comment on Opinion 2/2002 Art. 29 Data Protection Working Party

February 25th 2003

Brussels

Agenda.

- Who is the IPv6 Task Force?
- The issue
- The IPv6 Task Force Position

IPv6 Task Force Phase 1.

- IPv6 Task Force initiated by European Commission 2001
- Conclusions and recommendations of the Task Force submitted to the European Council Barcelona Spring meeting of 2002, under the Spanish Presidency
  - Recommendations pertaining to the implementation of IPv6 by all relevant ICT sectors.
  - Heads of State resolution to prioritize the deployment of the New Internet Protocol IPv6.
  - Communication from the Commission to the Council and the European Parliament “Next Generation Internet-priorities for action in migrating to the new Internet protocol IPv6”.

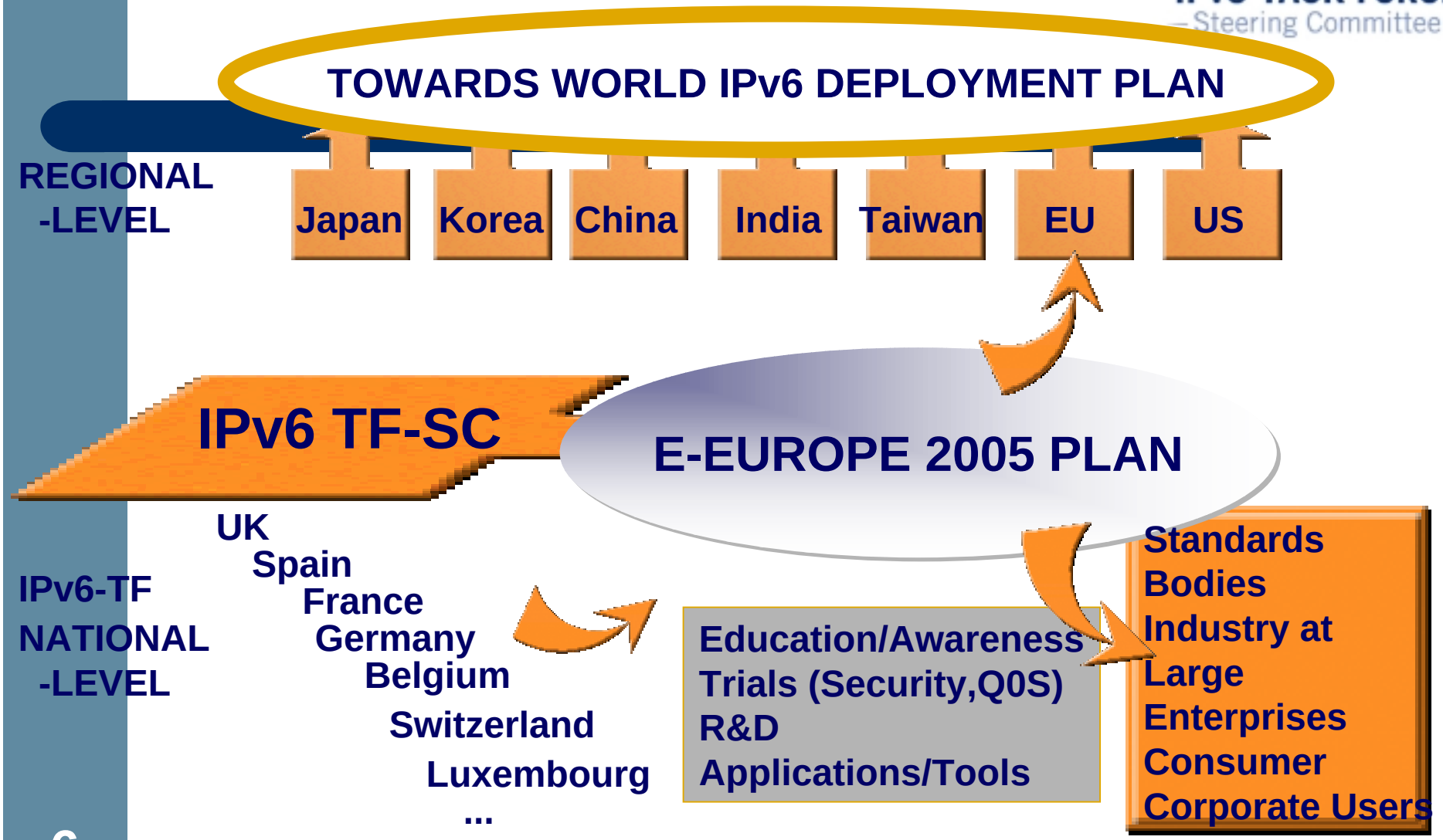
IPv6 Task Force Phase 2.

- Renewed mandate 2002-2004
- Ensure a working liaison of the European industries and Academia with standards and Internet governance bodies on IPv6.
- Provide a regularly updated review and plan action (“the European IPv6 Roadmap”) on the development and future perspectives of IPv6 in order to coordinate European efforts on IPv6.
- Establish collaboration arrangements and working relationships with similar initiatives being launched in other world regions.

IPv6 Task Force Steering Committee.

- Facilitate, support and coordinate the continuation of the work of the IPv6 Task Force until 2004.
- Strategic instrument to create ground for discussion and monitor how the recommendations are transformed.
- Collaborate with other regional groups and initiatives deploying IPv6.

IPv6TF-SC Actions.



Agenda.

- Who is the IPv6 Task Force?
- The issue
- The IPv6 Task Force Position

The issue.

- Document „Opinion 2/2002: on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6“.
- Released 30 May 2002 by the Article 29 Data Protection Working Party, set up under Article 29 of Directive 95/46/EC.
- Document describes the possible threats for privacy on the use of unique identifiers in telecommunication terminal equipments.
- Illustrates some of those concerns using as a concrete example the case of next generation protocol IPv6.

Agenda.

- Who is the IPv6 Task Force?
- The issue
- The IPv6 Task Force Position

The IPv6 TF Position.

- The EC IPv6 Task Force (EC IPv6 TF) recognizes that the use of unique identifiers in any kind of technology or communication media (e.g. Ethernet, WLAN, GSM, ID cards, IPv4, and IPv6) represents a potential threat for privacy.
- But the Task Force also notes that the use of stable identifiers is an important practical requirement in any communication system.

The IPv6 TF Position.

- The Task Force is concerned that the referred document,
  - which aims to create awareness about possible privacy threats in the development of the Internet.
- Can result in an unbalanced view of the benefits that can be obtained by adoption of IPv6, especially when compared to what exists now for IPv4.

The IPv6 TF Position.

- All communications are subject to privacy issues, and IPv6 is no exception.
- But IPv6 has provided a mechanism (RFC3041) that goes a long way to solving the problem, potentially providing a higher degree of protection to the users than is possible with IPv4.
  - RFC3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6.
- In addition, IP security (IPSec) mechanisms are available in full IPv6 implementations (RFC2460).
  - Although their use is not mandated, this offers an improvement over IPv4, where IPSec support is not present by default.

The IPv6 TF Position Technical Rationale.

- The following key considerations must be taken in account when reviewing the privacy implications with IP-based communications, both for the existing IPv4 and the emerging IPv6.

1. IPv4 has privacy issues with static IP addresses being used as identifiers. These can be tracked just as other devices and items used by a person can be.

The IPv6 TF Position Technical Rationale.

2. IPv6 by default where stateless autocofiguration is used will construct IPv6 addresses that allow correlation of activity where the same device is connected to different networks, because a constant identifier (based on hardware in the device) is embedded in the IPv6 address.

3. RFC3041 fixes the problems of correlation by allowing an IPv6 device to generate a random identifier to embed in the address.

The IPv6 TF Position Technical Rationale.

4. IPv6's Privacy Extensions enable a static host (e.g. workstation in an office) to use different IPv6 source addresses through time (e.g. a different IPv6 source address daily), allowing greater privacy for such non-mobile devices and users.

5. It is normal practice for IPv6 devices to have multiple addresses, where IPv4 devices usually have one address. It is thus possible for future IPv6 applications to use multiple (dynamic) IPv6 addresses, e.g. to reduce traceability in peer-to-peer applications.

The IPv6 TF Position Technical Rationale.

6. Many Internet systems use IP addresses as a (weak) authentication mechanism. Use of Privacy Extensions prevents such authentication being used. However, IPv6 includes IPSec by default, allowing stronger authentication methods to be used.

7. Further research may introduce new classes of IPv6 addresses, for example cryptographically generated addresses. This is only possible with IPv6.

The IPv6 TF Position Technical Rationale.

8. The EC IPv6 TF strongly recommends that vendors implement RFC3041 by default in all systems. The TF notes that some vendors have already done so.

9. There should be easy user-controllable mechanisms for RFC3041 to be enabled or disabled, per device/interface or per application.
   - This could also be automatic depending on the initiated traffic (in-bound or outbound), pre-configured by default or customized.
   - These may require further work or research.
   - Again, such enhancements are only possible with IPv6.

Summary.

- The EC IPv6 TF believes that the new built-in properties in IPv6 provide a set of necessary and unique tools to empower a user's privacy in ways that are not possible in IPv4.

- The combination of the availability of IPSec support in full IPv6 implementations combined with these new properties makes IPv6 a potentially powerful tool to improve the possibilities for user privacy.

Summary.

- The TF strongly recommends the implementation of RFC3041 by all IPv6 vendors.
- However, it is clear that in any communication medium a balance needs to be struck between usability and privacy.
- For example, further work would be desirable on allowing user-controllable enabling of the IPv6 privacy extensions on a per-application basis.

Summary.

- The IPv6TF asks the Article 29 Data Protection Working Party to consider the above mentioned issues.
  - A written statement has been provided (http://www.ec.ipv6tf.org/PublicDocuments/Article29_v1_2.pdf)
- The IPv6TF SC asks the Article 29 Data Protection Working Party to reconsider its statement on IPv6 as a the possible threats for privacy, taking into account the significant improvements that have been included in IPv6 with respect to privacy and data protection.
- For the IPv6 community who has observed the statement with concern, this would be an important signal.

More http://www.ipv6tf.org Contact.

Dr. André Zehl
Project Leader IPv6 Task Force – Steering Committee

Deutsche Telekom Group
T-Systems
Goslarer Ufer 35
10589 Berlin
Germany
Tel. +49 30-3497-3126
Fax +49 30-3497-3127
andre.zehl@t-systems.com

Annex: Privacy Extensions for Stateless Address Autoconfiguration (RFC3041).