

MPHPT

March 17, 2003, Vol. 13, No. 23

*Please feel free to use the articles in this publication, with proper credits*

## COMMUNICATIONS NEWS

Biweekly Newsletter of the Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan

# APT Conference Preparatory Group Meeting for ITU World Radiocommunication Conference

The World Radiocommunication Conference (WRC) of ITU has been convened every two or three years with the main purpose of amending the Radio Regulations that stipulate international frequency allocation, etc. The next Conference, WRC-03, will be held for considering about forty items, including 5-GHz wireless access systems and Systems beyond IMT-2000 for four weeks from June 9, 2003, in Geneva, Switzerland.

As efforts to address WRC-03, the Asia-Pacific Telecommunity (APT) in the Asia-Pacific region has been holding the APT Conference Preparatory Group (APG) Meeting for WRC-03. From February 19 through 25, 2003, the 5th APG Meeting for WRC-03 (the final meeting) was held in Shinjuku, Tokyo. At the meeting, with about 370 participants representing 25 Member States, Associate Members, Affiliate Members, Participating Companies of APT and international/regional organizations in attendance, the Preliminary APT Common Proposals (PACPs) were adopted.

## (1) Introduction of radio LANs into 5150-5350 MHz and 5470-5725 MHz bands

As regards introduction of radio LANs into 5150-5350 MHz and 5470-5725 MHz bands, a PACP was formulated for primary allocations of 5150-5350 MHz (indoor use) and 5470-5725 MHz (outdoor use) bands to mobile service.

## (2) Consideration of future development of IMT-2000 and systems beyond IMT-2000

With respect to systems beyond IMT-2000, a PACP was formulated for identifying frequencies at WRC-07.

## (3) Consideration of the provisions concerning the Stratospheric Radio Platforms (high altitude platform stations: HAPS) and the additional frequencies

Within 31.0-31.3 GHz band additionally specified to HAPS at WRC-2000, a PACP was formulated for enabling use of 31.15-31.3 GHz band, currently limited in use, through introduction of criteria and coordination procedures for protecting adjacent band (Earth exploration-satellite service (passive) and radio astronomy service in 31.3-31.8 GHz band).

## (4) Identification of frequencies for public protection and disaster relief (PPDR)

For communications among public organizations responding to public protection, disaster relief, emergencies, etc., a PACP was formulated for i) identifying six frequency bands, including 440-470 MHz band which Japan supports, as globally/regionally harmonized frequency bands, and ii) as regards methods for frequency use, allowing, at the administration's discretion, the continued use of the identified bands for other services.

## (5) Consideration of provisions on highly elliptical orbit (HEO) satellite networks

With regard to a PACP for adding power flux density limit values suitable for HEO systems, which will enable sharing with geostationary satellite systems in 19.7-20.2 GHz band, it was decided to await outputs of ITU-R SG4 meeting following this APG meeting.

## (6) Review of procedures and sharing

criteria for broadcasting satellite service (BSS) plan

With regard to interference criteria between BSSs, a PACP was formulated for protecting reception by antennas with diameter of 45 cm exclusively for those countries already using the antennas for domestic broadcasting, and reception by antennas with diameter of 60 cm in other countries.

## CONTENTS

- APT Conference Preparatory Group Meeting for ITU World Radiocommunication Conference (WRC) ----- 1
- Holding of "Study Group Concerning Information Privacy in the Telecommunications Business Field"<sup>2</sup>
- Final Report of "Study Group on Broadcasting Policy" (Outline) ----- 2
- "List of the e-Government recommended cryptographic techniques" Adopted ----- 4

**International Policy Division,  
International Affairs Department,  
Ministry of Public Management, Home  
Affairs, Posts and Telecommunications  
1-2, Kasumigaseki 2-chome,  
Chiyoda-ku, Tokyo 100-8926, Japan**

• We welcome your comments via:  
[feedback-newsletter@soumu.go.jp](mailto:feedback-newsletter@soumu.go.jp)  
Fax: +81-3-5253-5924  
Tel.: +81-3-5253-5920

• MPHPT information is available at:  
<http://www.joho.soumu.go.jp/eng/>

Preliminary APT Common Proposals | adopted this time are to be submitted to | Member States.  
WRC-03 after approval procedures by

# Holding of "Study Group Concerning Information Privacy in the Telecommunications Business Field"

MPHPT convened the "Study Group concerning Information Privacy in the Telecommunications Business Field" in order to obtain opinions from a wide range of stakeholders and deliberate upon the handling of personal data in the telecommunications business field. The first meeting was held on February 24, 2003.

In the telecommunications business field, from the nature of its business a large amount of information related to personal data including the secrecy of communications is handled. As per usual, there have been calls for such information to be handled appropriately. Therefore, in the networked society where digitized information is distributed at high speed over networks, there has been a rise in interest as regards the handling of personal data and led to the

current debate concerning legal frameworks on personal information protection, etc.

On the other hand, recently with the widespread use of the Internet and mobile telephony, damages from misuses of telecommunications media have been occurring and are leading to debates as to the protection of privacy-related information from a variety of standpoints.

The protection of privacy-related information has also been discussed in many countries and some international organizations (such as discussions at OECD concerning the eight Principles of Privacy Guidelines).

In light of the above situation, regarding the processing of personal data in the telecommunications business field, in addition to investigating the trends at home and abroad, it was decided that

deliberations upon measures for processing personal data based upon hearings on opinions from a wide range of stakeholders are to be conducted.

## [Items to be deliberated upon]

1. The current status in protection of secrecy of communications and personal data
2. Measures for dealing with individual cases
3. Desirable processing of personal data possessed by telecommunications carriers, taking into consideration the bill for protecting personal information

## [Schedule]

Following the first meeting on February 24, 2003, the Study Group will compile its findings by spring of 2004.

# Final Report of "Study Group on Broadcasting Policy" (Outline)

## -- Review of Media Ownership Rule --

Since May 2000, MPHPT has been holding the "Study Group on Broadcasting Policy" (Chair: Prof. SHIONO Hiroshi, Department of Correspondence Graduate Studies, University of East Asia) with the objective of studying overall broadcasting policies based on the changing environment surrounding broadcasting, including the progress of digitalization in all broadcasting media and the advancement of the Internet. After a series of meetings, the Study Group compiled its findings as the "final report" centering on the principle of media ownership rule.

The outline of the final report is as follows:

### I. Situation surrounding broadcasting

As a prerequisite for deliberating upon the desirable "principle of media ownership rule," centering on points pertaining to scarcity of frequency resources and social influence of broadcasting, this part scrutinizes recent changes in media environments and prospects development trends of future terrestrial and satellite broadcasting, broadcasting and broadband communications.

### II. The desirable "principle of media ownership rule"

1. The "Principle of media ownership

rule" and its policy purposes: it is appropriate to make "plurality," "diversity" and "localism" important policy purposes to be continuously attained.

2. Adequacy concerning the review of the existing "principle of media ownership rule": The changing environment surrounding the media is to be highlighted, in particular, the availability of increased choices for viewers/listeners to obtain information. Taking into consideration these points, it is basically enough to relax appropriately the existing "principle of media ownership rule."

### III. Practical directions of review on the existing "principle of media ownership rule"

#### 1. Terrestrial broadcasting

- (1) Deregulation within the same broadcasting service area and between different broadcasting service areas: In comparison with deregulation between different service areas (the current limitation on "less than one-fifth" of voting rights), deregulation within the same service area shall be carefully dealt with (the current limitation on "one-tenth" of voting rights or less).
- (2) Deregulation between different broadcasting service areas: In cases of deregulation between key stations and local stations, deregulation shall be carefully deliberated upon within the scope in which the local features of local stations cannot be deteriorated (with regard to regulations on capital ratio, deregulation shall be limited to the "maintenance of the status quo" or "minor deregulation.").
- (3) Practical deregulation between local stations: Upon deregulation between local stations, where one of the important purposes of terrestrial broadcasting, "localism," is maintained. Meanwhile the business basis is strengthened in order to be conducive to digitalization and to improvement in capacities, to produce localism-based programming and transmitting localism-based information,
  - a) Between broadcasters who comply with "certain conditions taking into consideration the local features" ((i) a broadcast service area adjacent to another broadcasting service area, and (ii) lim-

ited to 2 broadcasting service areas), it is appropriate to introduce major deregulation, for instance, "cross-ownership of two or more media (or wholly-owned subsidiaries)."

- b) In cases where the conditions above are not met, "cross-ownership of two or more businesses (or wholly-owned subsidiaries)" shall not be allowed. With regard to regulations on capital ratio, however, it is sufficient that deliberations on a certain level of deregulation concerning the regulated capital ratio between local stations, in line with the degree of local features, be introduced.

Notes: 1. In Japan, under the Broadcast Law, a "broadcasting service area" (a fixed area deemed appropriate for receiving simultaneously the same broadcast programs) is set forth in which broadcasting is being carried out. Under the current regulatory frameworks, the upper limit of capital ratio for a broadcasting station within the same broadcasting service area (one-tenth of voting rights or less) and that for a broadcasting station between different service areas (less than one-fifth of voting rights) differ from each other.

2. A "key station" means a large-scale broadcaster which broadcasts in major metropolitan area. A "local station" means a broadcaster which broadcasts in local areas.

#### 2. Satellite broadcasting

- (1) Adequacy of cross-ownership of BS digital broadcasting and terrestrial broadcasting: It is inappropriate that with regard to BS digital broadcasting, cross-ownership between terres-

trial broadcasting be approved.

- (2) Adequacy of relaxation of the regulations on capital ratio: From the viewpoints of maintaining pluralism in broadcasting, it is appropriate to relax the regulations on capital ratio.
- (3) Practical measures for reviewing the current regulatory frameworks on BS digital broadcasting: It is appropriate to relax the current upper limit of capital investment from "less than one-third of voting rights" to "one-half of voting rights or less."

#### 3. On continuity of broadcasting services – treatment of broadcasters which are in difficulty of management --

In cases where a broadcaster is in difficulty of continuing broadcasting services, from the viewpoint of ensuring benefits of viewers/listeners, it is appropriate to approve drastic and exceptional relaxation for ensuring continuity of broadcasting services under a certain condition.

#### IV. Matters to be deliberated upon other than the "principle of media ownership rule"

Considering matters of interest presented by members of the Study Group, in order to contribute to the future broadcasting administration, the following four items were deliberated upon as challenges: "Concept of broadcasting," "On Japan Broadcasting Corporation (NHK)'s business operations (based upon the First Report)," "On community-based broadcasting and broadcasting networks" and "On public scheme for production/distribution of broadcast programming."

# "List of the e-Government recommended cryptographic techniques" Adopted

By 2003, the realization of the "e-Government" that makes administrative procedures possible via information and communication systems in principle from home or office is being scheduled.

In order to establish e-Government that citizens can access securely, it is vital that the information security of the e-Government be assured. For this, as regards cryptographic techniques constituting a core technology of information

security, it is essential to use cryptographic techniques meeting a high level of security and reliability, and said security and reliability need to be results of objective evaluations.

Thus, MPHPT and the Ministry of Economy, Trade and Industry (METI) have been conducting a project for evaluating cryptographic techniques, called the "Cryptography Research and Evaluation Committees (CRYPTREC)"

project, through activities of the "CRYPTREC Advisory Committee" (Chair: Professor IMAI Hideki, the University of Tokyo) jointly with the "CRYPTREC Evaluation Committee" (Chair: Professor IMAI Hideki; held by the Telecommunications Advancement Organization of Japan: TAO and the Information-technology Promotion Agency, Japan: IPA). Under the CRYPTREC project, cryptographic

The list of the e-Government recommended cryptographic techniques

Technical classification		Name
Public-key cryptographic techniques	Signature	DSA ECDSA RSASSA-PKCS1-v1_5 RSA-PSS
	Confidentiality	RSA-OAEP RSAES-PKCS1-v1_5 *1
	Key agreement	DH ECDH PSEC-KEM *2
Symmetric-key cryptographic techniques	64-bit Block ciphers *3	CIPHERUNICORN-E Hierocrypt-L1 MISTY1 3-key Triple DES *4
	128-bit Block ciphers	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000
	Stream ciphers	MUGI MULTI-S01 128-bit RC4 *5
Related other techniques	Hash functions	RIPEND-160 *6 SHA-1 *6 SHA-256 SHA-384 SHA-512
	Pseudo-random number generators *7	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1 PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1 PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

\*1: accepted in the present use according to the actual result in SSL3.0 or TLS1.0

\*2: supposed to be used on the condition of KEM-DEM construction

\*3: 128-bit block ciphers should be selected if longer block length ciphers could be suited and used for the systems on the occasion of construction of new e-Government systems.

\*4: accepted in the present use on the following conditions

- 1) to be specified in FIPS46-3
- 2) to keep the status of de facto standard

\*5: supposed to be used in the limited usage in the version of more than SSL3.0 or TLS1.0. If the other ciphers listed in the table could be used, they should be selected.

\*6: More than 256-bit hash functions should be selected if longer hash functions could be suited and used for the systems on the occasion of construction of new e-Government systems. Provided that a hash function is specified in the public-key cryptography to be used, there is nothing like this.

\*7: Use of any generators has fundamentally no problem if cryptographically secure algorithms would be used, in accordance with no needs for interconnectivity. These published PRNGs are sample cases.

technique submissions were publicly invited, and evaluated cryptographic techniques were proposed. On February 20, 2003, the "List of the e-Government recommended cryptographic techniques" was decided for use in the government procurement of the e-Government systems.

Further, the guidelines for using cryp-

tographic techniques in information system procurement by the relevant office and ministries were agreed to upon the recommendation that, in cases where the relevant office and ministries use cryptographic techniques upon construction of information systems, whenever possible the relevant office and ministries shall employ cryptographic techniques

in the "List of the e-Government recommended cryptographic techniques."

From FY2003, MPHPT, jointly with METI, will continuously monitor the security and reliability of the e-Government recommended cryptographic techniques, and if necessary, will evaluate cryptographic techniques and provide information thereon.