Overview of CRYPTREC Activities

January 28, 2002

Hideki Imai, Professor, University of Tokyo,
CRYPTREC Advisory Committee Chair,
CRYPTREC Evaluation Committee Chair

Summary of CRYPTREC Activities

- **Activities intended to establish a cryptographic technique evaluation system in Japan**
- **Evaluation of cryptographic techniques in terms of their applicability to e-government**
- **Support of standardization activities**

Fairness and transparency of activities
(Descriptions of evaluation activities are made public on the Internet.)

Cryptographic techniques applicable to e-government

Application period of cryptographic techniques usage policy:

Approximately 10 years

Types of e-government systems

Systems relating to government services involving the private sector

Regional public organizations are also considered.

International standards

Cooperation with ISO/IEC, NESSIE, AES, etc.

Interoperability and security

Cipher application categories and number of recommended ciphers

Other issues to consider

Guidebook for system procurement, etc.

Cryptographic techniques to be evaluated

- **Cryptographic techniques submitted in response to FY2000 call**
- **Cryptographic techniques submitted in response to FY2001 call**
- **Cryptographic techniques considered necessary for evaluation by Advisory Committee and Evaluation Committee**

Categories of ciphers to be evaluated

Asymmetric-key ciphers

(combinations of cryptographic schemes and cryptographic primitives)

- **Confidentiality, authentication, signature, key agreement**

Symmetric-key ciphers

- **Stream ciphers**
- **64-bit block ciphers, 128-bit block ciphers**

Hash functions

Pseudo-random number generators

Steps in evaluating cryptographic techniques

Screening evaluation

Evaluation to screen for full evaluation

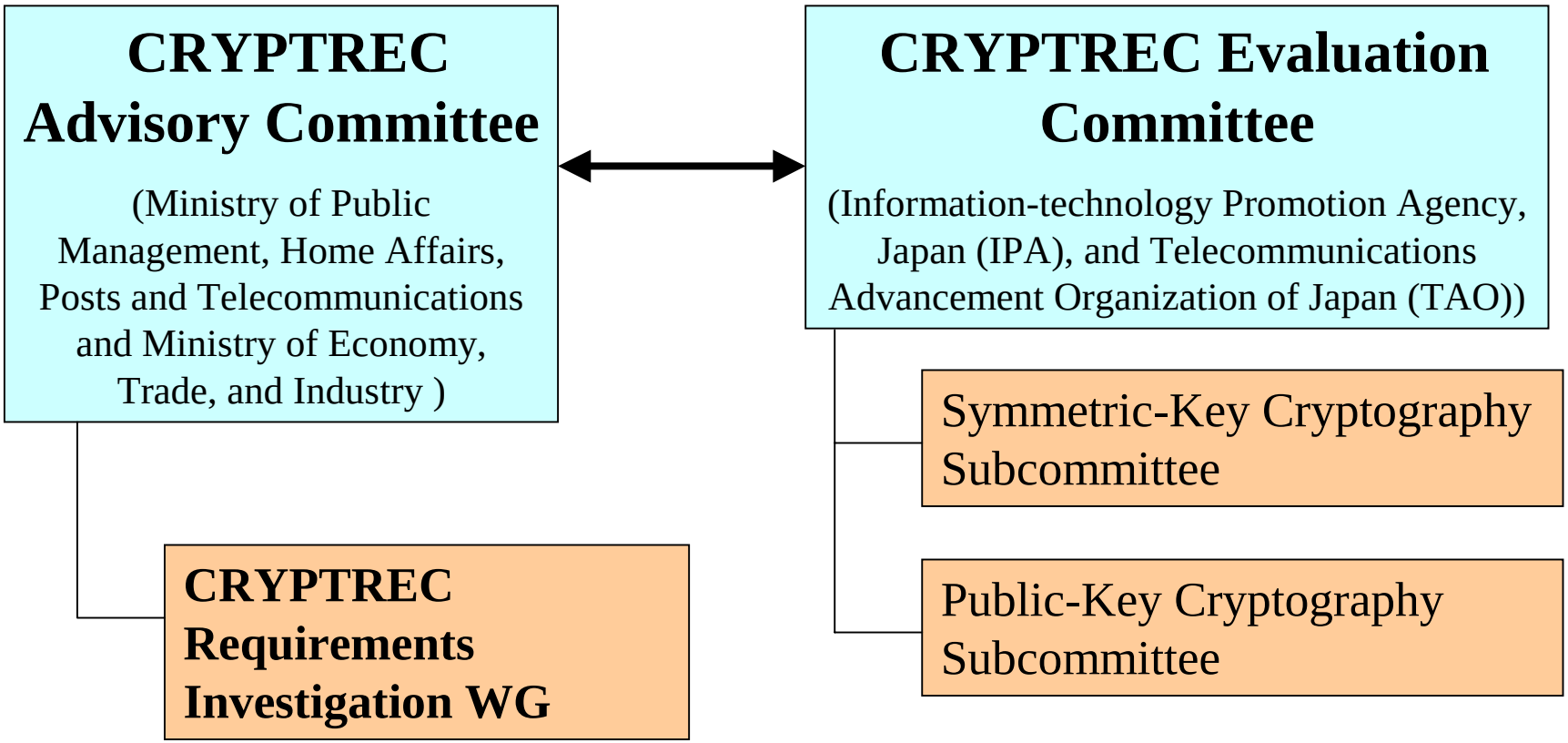
- First evaluation to determine whether there are trivial security problems
- First evaluation to determine whether it can be implemented by a third-party

Full evaluation

Evaluation to determine usability for e-government

- Consolidated evaluation using known attack methods
- Strength evaluation of individual candidate ciphers (Attack)
- Evaluation to determine whether there are problems related to parameter/key setting criteria
- Software implementation evaluation

CRYPTREC System



CRYPTREC Advisory Committee
(focused on examination of political issues)

Committee Chair Hideki Imai

CRYPTREC Requirements Investigation WG Chair:

Ryoichi Sasaki

- **Preparation of usage policy draft for e-government recommended ciphers**
- **Arrangement of cryptographic technique requirements**
- **Study of how cipher evaluations should be in the future**

Administrative offices:

Ministry of Public Management, Home Affairs, Posts and Telecommunications, and Ministry of Economy, Trade, and Industry

CRYPTREC Advisory Committee Members

Committee Chair: Hideki Imai	University of Tokyo
Adviser: Shigeo Tsujii	Chuo University
Jun Ikimune	Japan Information Technology Service Industry Association
Naoyuki Iwashita	Institute for Monetary and Economic Studies, Bank of Japan
Hiroshi Okazaki	Communications Industry Association of Japan
Eiji Okamoto	Toho University
Tatsuaki Okamoto	Nippon Telegraph and Telephone Corporation
Yoshifumi Kato	Telecom Services Association
Toshinobu Kaneko	Science University of Tokyo
Akio Kokubu	New Media Development Association
Koichi Sakurai	Kyushu University
Ryoichi Sasaki	Tokyo Denki University
Kazuo Takaragi	Japan Electronics and Information Technology Industries Association
Kenji Naemura	Keio University
Mitsuru Matsui	Mitsubishi Electric Corporation
Tsutomu Matsumoto	Yokohama National University, Graduate School

CRYPTREC Evaluation Committee (focus on technology evaluations)

Hideki Imai, CRYPTREC Evaluation Committee Chair

Tsutomu Matsumoto, Public-Key Cryptography Subcommittee Chair

Toshinobu Kaneko, Symmetric-Key Cryptography Subcommittee Chair

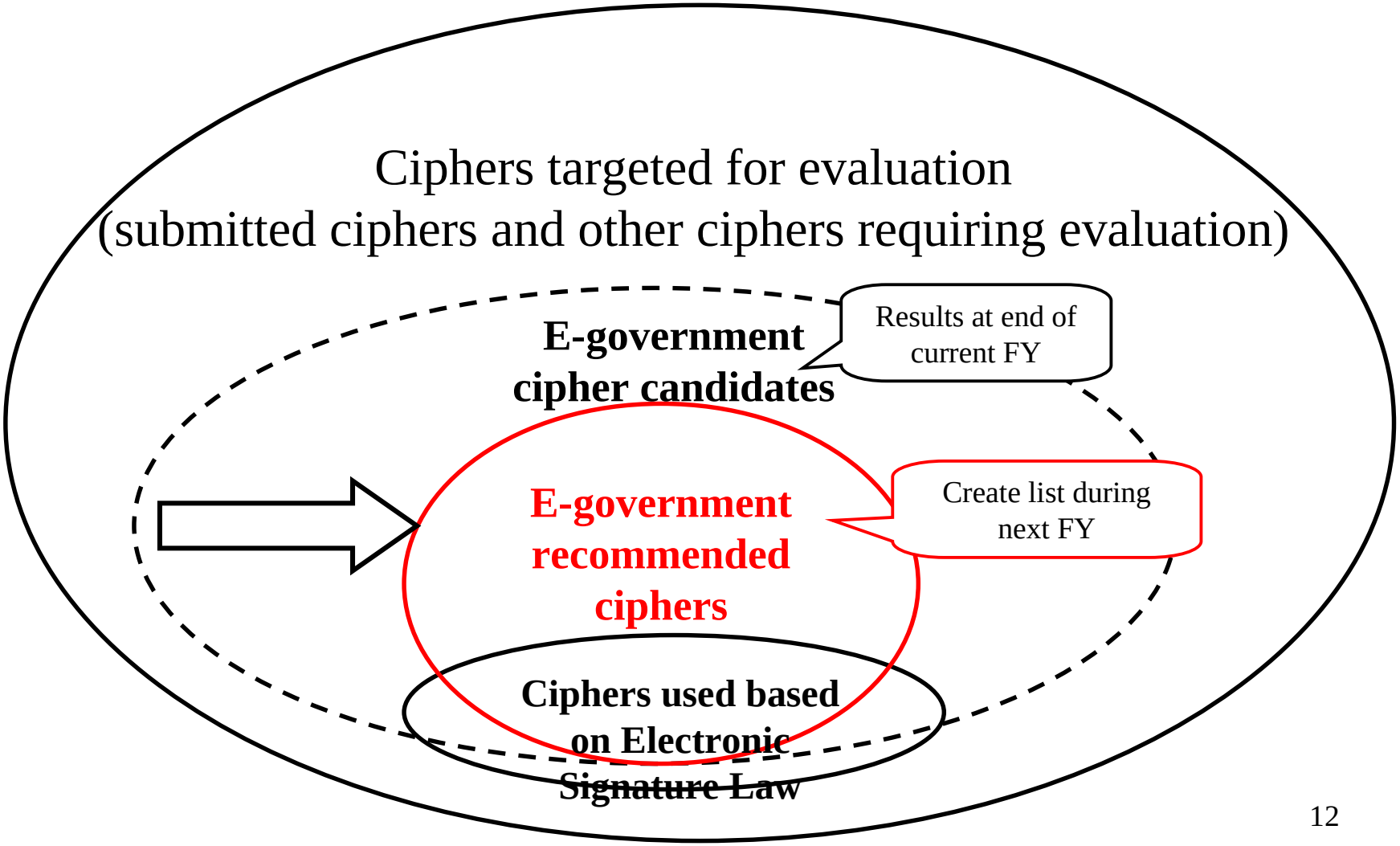
- **Study of evaluation methods for individual cryptographic technique categories**
- **Evaluation of cryptographic techniques submitted in response to call**

Administrative offices: Information-technology Promotion Agency, Japan, and Telecommunications Advancement Organization of Japan

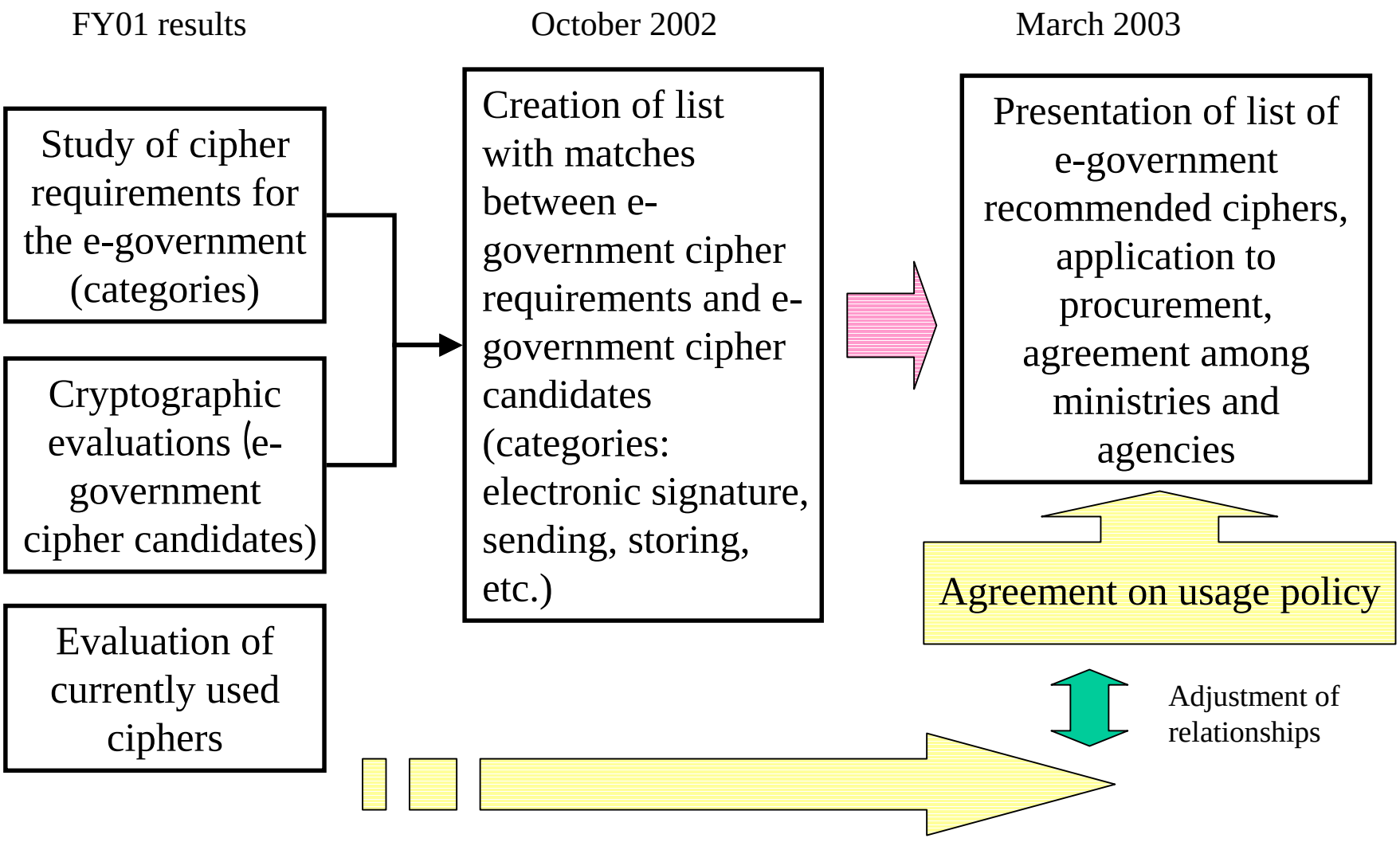
CRYPTREC Evaluation Committee Members

Committee Chair	**Hideki Imai**	**University of Tokyo**
Adviser	**Shigeo Tsujii**	**Chuo University**
Member	**Eiji Okamoto**	**Toho University**
Member	**Tatsuaki Okamoto**	**Nippon Telegraph and Telephone Corporation**
Member	**Toshinobu Kaneko**	**Science University of Tokyo**
Member	**Mitsuru Matsui**	**Mitsubishi Electric Corporation**
Member	**Tsutomu Matsumoto**	**Yokohama National University, Graduate School**

E-government recommended ciphers



Schedule for studying e-government recommended ciphers



Toward e-government in 2003

FY2000

Establishment of CRYPTREC Evaluation Committee

- **Call for e-government cryptographic techniques**
- **Evaluation of e-government cryptographic techniques (screening evaluation and full evaluation)**

FY2001

Establishment of CRYPTREC Advisory Committee

- **Study on what cipher evaluations should be**
- **Arrangement of cryptographic technique requirements for e-government**

CRYPTREC Evaluation Committee

- **Second call for e-government cryptographic techniques**
- **Evaluation of e-government cryptographic techniques (screening evaluation and follow-up evaluation)**

Toward e-government in 2003 (cont'd)

Activity plans for FY2002

Selection of e-government recommended ciphers

Arrangement of requirement study categories and cryptographic technique evaluation categories

Guidebook for e-government system procurement

CRYPTREC Advisory Committee

Finalization of cryptographic technique requirements

CRYPTREC Evaluation Committee

Evaluation of e-government cryptographic techniques (full evaluation and follow-up evaluation)

No plans for a new call for candidates in FY2002

Publication schedule of this fiscal year's reports

April 16, 2002 CRYPTREC 2001-2001

CRYPTREC Advisory Committee Report

CRYPTREC Evaluation Committee Report

CRYPTREC Report 2001

(FY2001 evaluation report

and cryptographic techniques specifications)

Cryptographic techniques application guidelines

Future challenges

Information required for e-government system procurement

- Publish as JIS-TR
- Guidebook for cryptographic techniques procurement
- Cipher implementation protocols and module evaluations

Permanent evaluations by neutral, public institution

International collaboration

- Cooperation with AES, ISO/IEC, NESSIE, etc.

Comments Welcome

We welcome your comments on the cryptographic techniques being evaluated.

Email address

cryptrec-comment@ipa.go.jp

For further information, visit the CRYPTREC homepage:

IPA :http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html

TAO :http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index-e.html