CRYPTREC Project 2001

Hideki Imai

Chair, CRYPTREC Evaluation Committee

Institute of Industrial Science,
the University of Tokyo

http://imailab-www.iis.u-tokyo.ac.jp/

CRYPTREC

（Cryptography Research & Evaluation Committee）

- **CRYPTREC**
  - Founded in April 2000
  - In 2001, Sponsored by

    Ministry of Public Management, Home Affairs,
    Posts and Telecommunications

    Ministry of Economy, Trade and Industry
- **CRYPTREC Project**
  - Open call for cryptographic techniques
  - Evaluation
  - Publishing the technical report

Foundations of CRYPTREC

- **Project of the Information-Technology Promotion Agency (IPA), JAPAN**
  - Investigation and research on criteria for cryptography to be procured by the government
- Study Group for Promotion and Advancement of Encrypted Communications, MPT
- Project of Telecommunications Advancement Organization of Japan (TAO)

⇨ CRYPTREC Project

This project was a part of the Electronic Government Security Technology Development Project, which was sponsored by MITI and entrusted to the Information-technology Promotion Agency (IPA), Japan.

Motivation of CRYPTREC Project (1)

- Creation of the infrastructure for the e-government by FY 2003
- Assessment of the security and the implementation of available cryptographic techniques to achieve information security in the e-government
- Enhancing the security and reliability of the nationwide information network

Motivation of CRYPTREC Project (2)

- **Recommendation of the OECD Council "Guidelines for Cryptography Policy"**
  - **PRINCIPLES 1. TRUST IN CRYPTOGRAPHIC METHODS**
    - Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.
- **Trend of the Cryptographic Standardization**
  - **ISO/IEC JTC1 SC27**
    - **From registration (IS-9979) to real standard**
  - **AES Project in USA**
  - **NESSIE (New European Schemes for Signature, Integrity, and Encryption)**
    - **The Information Societies Technology (IST) Programme of the European Commission**

Goals of CRYPTREC Project

- **Open call for cryptographic techniques**
  - Proposed cryptographic techniques are evaluated from a technical point of view by experts
- **Listing the cryptographic techniques which can be used for the e-government**
  - The report will be submitted to the government and open to the public
- **A step to establishing an organization for cryptographic technology evaluation in JAPAN**

Categories of Solicited Cryptographic Techniques

- **Asymmetric Cryptographic Schemes**
  - Asymmetric cryptographic schemes possessing one of the following objectives are solicited:
    - Confidentiality;
    - Signature;
    - Authentication; and
    - Key agreement
- **Symmetric Ciphers**
  - Stream ciphers , 64-bit block ciphers, 128-bit block ciphers
- **Hash Functions**
- **Pseudo-Random Number Generators**

Features of CRYPTREC Project

- **Related government offices participate in CRYPTREC as observers:**
  - Cabinet Office *
  - National Police Agency*
  - Japan Defense Agency *
  - Ministry of Public Management, Home Affairs, Posts and Telecommunications *
  - Ministry of Justice *
  - Ministry of Foreign Affairs of Japan
  - Ministry of Finance *
  - Ministry of Economy, Trade and Industry *

(* : Since 2000)

- **Front-line researchers in the area of cryptology in Japan assembled**

Features of CRYPTREC Project

CRYPTREC

Related Government Offices

Front-line Researchers

CRYPTREC in FY 2001: Committees

- **Advisory Committee**
  - **Secretariat**

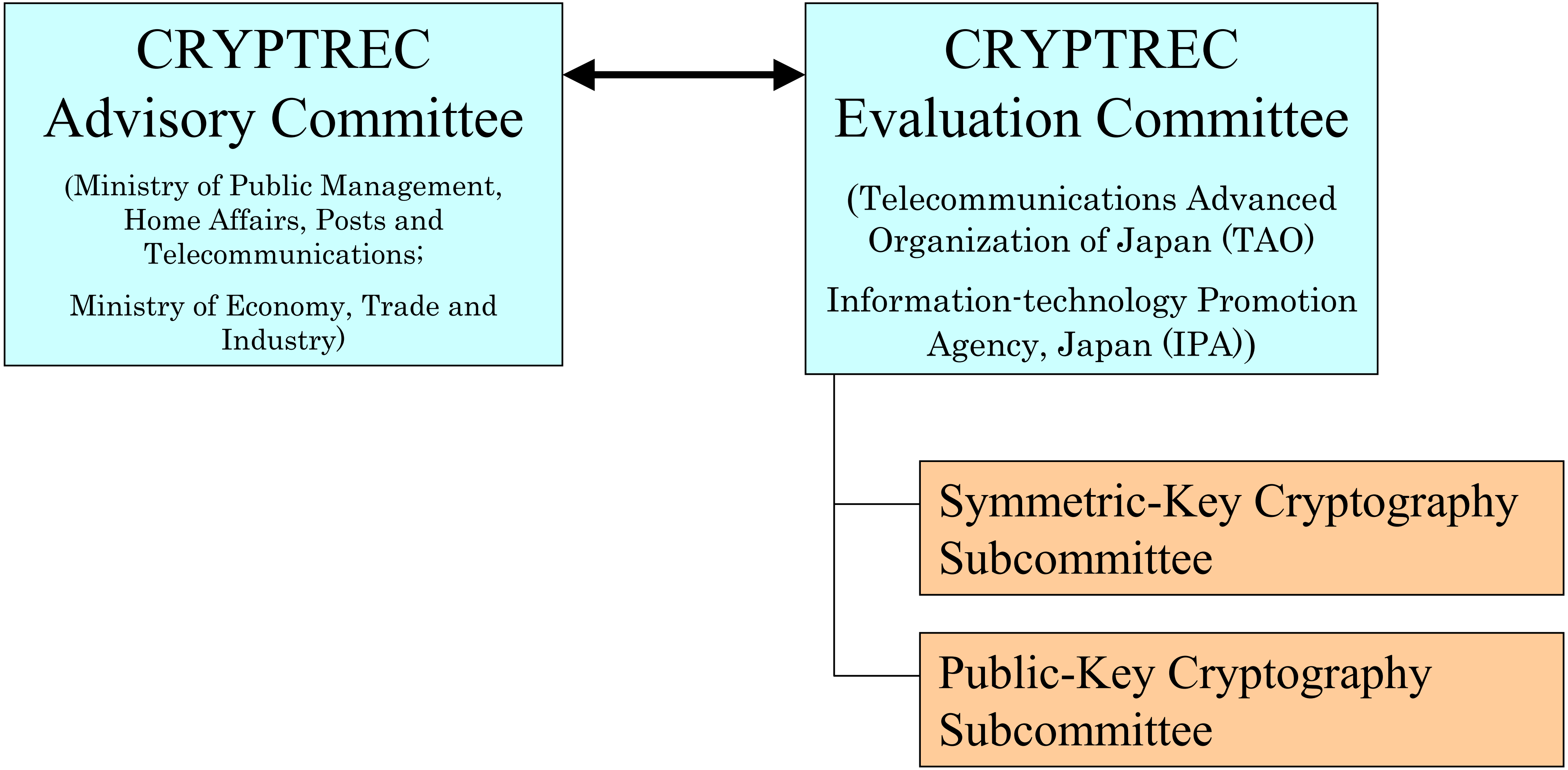
    - Ministry of Public Management, Home Affairs,

      Posts and Telecommunications;

    - Ministry of Economy, Trade and Industry
- **Evaluation Committee**
  - **Secretariat**

    - Telecommunications Advancement Organization of Japan (TAO);
    - Information-Technology Promotion Agency, JAPAN (IPA)

CRYPTREC Committees



CRYPTREC
Advisory Committee

(Ministry of Public Management, Home Affairs, Posts and Telecommunications;

Ministry of Economy, Trade and Industry)

CRYPTREC
Evaluation Committee

(Telecommunications Advanced Organization of Japan (TAO)

Information-technology Promotion Agency, Japan (IPA))

Symmetric-Key Cryptography Subcommittee

Public-Key Cryptography Subcommittee

Roles of the Committees

- CRYPTREC Advisory Committee

  (Examination of Political Issues)

  - Cryptographic guideline for e-government
  - Arrangement of technical requirements
  - Future cryptographic evaluation as it ought to be

- CRYPTREC Evaluation Committee

  (Technical Evaluation)

  - Evaluation criteria
  - Technical evaluation

CRYPTREC in FY 2001: Activities

- Investigating and Arranging Cryptographic Requirements (for e-Government)
- Evaluating Cryptographic Techniques
  - General Evaluation
  - Specific Evaluation
- Making a Cryptographic Guideline for Users

General Evaluation

- Screening Evaluation (FY 2001):

  Newly submitted cryptographic techniques in FY 2001 are evaluated as a first phase of evaluation.

- Full Evaluation (FY 2002):

  Newly submitted cryptographic techniques in FY 2001 that pass the screening evaluation will advance to the full evaluation phase, in which more detailed evaluation is executed by inspecting weaknesses in detail and performance etc., in FY 2002.

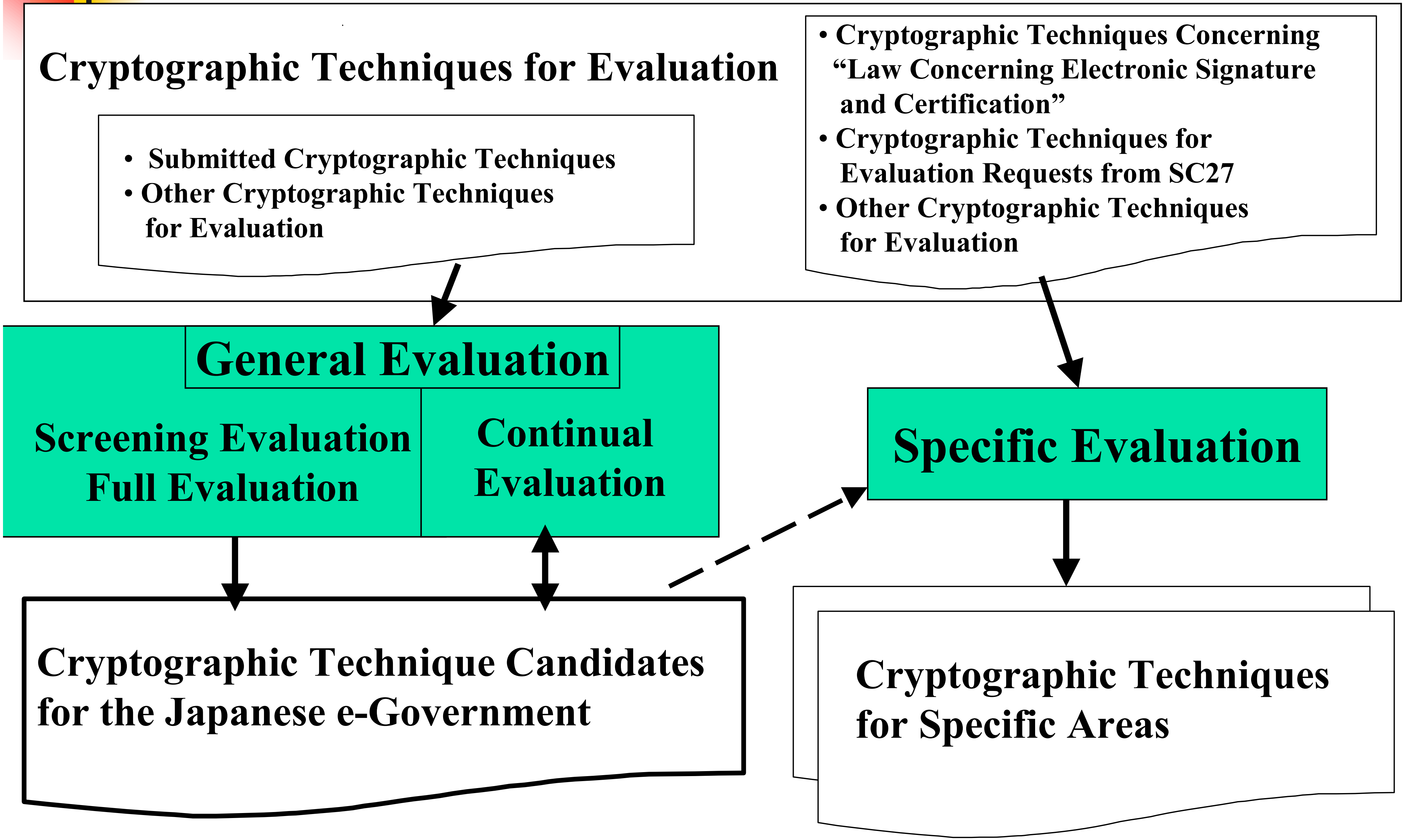
- Continual Evaluation (FY 2001)

  The techniques that were evaluated and concluded to be further evaluated in FY 2000 are evaluated. Furthermore, techniques that were evaluated in FY 2000 may be evaluated due to a recent trend.

Specific Evaluation

- The committees evaluate the cryptographic techniques requested by another organization and the techniques that the committees consider more detailed evaluation is necessary for a specific use.
- Specific evaluation in FY 2001 includes:
  - Evaluation of cryptographic techniques requested from the ISO/IEC JTC1 SC27 committee; and
  - Evaluation of digital signature schemes concerning "Law Concerning Electronic Signatures and Certification"

Image of Evaluation



Cryptographic Techniques for Evaluation

- Submitted Cryptographic Techniques
- Other Cryptographic Techniques for Evaluation

- Cryptographic Techniques Concerning "Law Concerning Electronic Signature and Certification"
- Cryptographic Techniques for Evaluation Requests from SC27
- Other Cryptographic Techniques for Evaluation

General Evaluation

Screening Evaluation
Full Evaluation

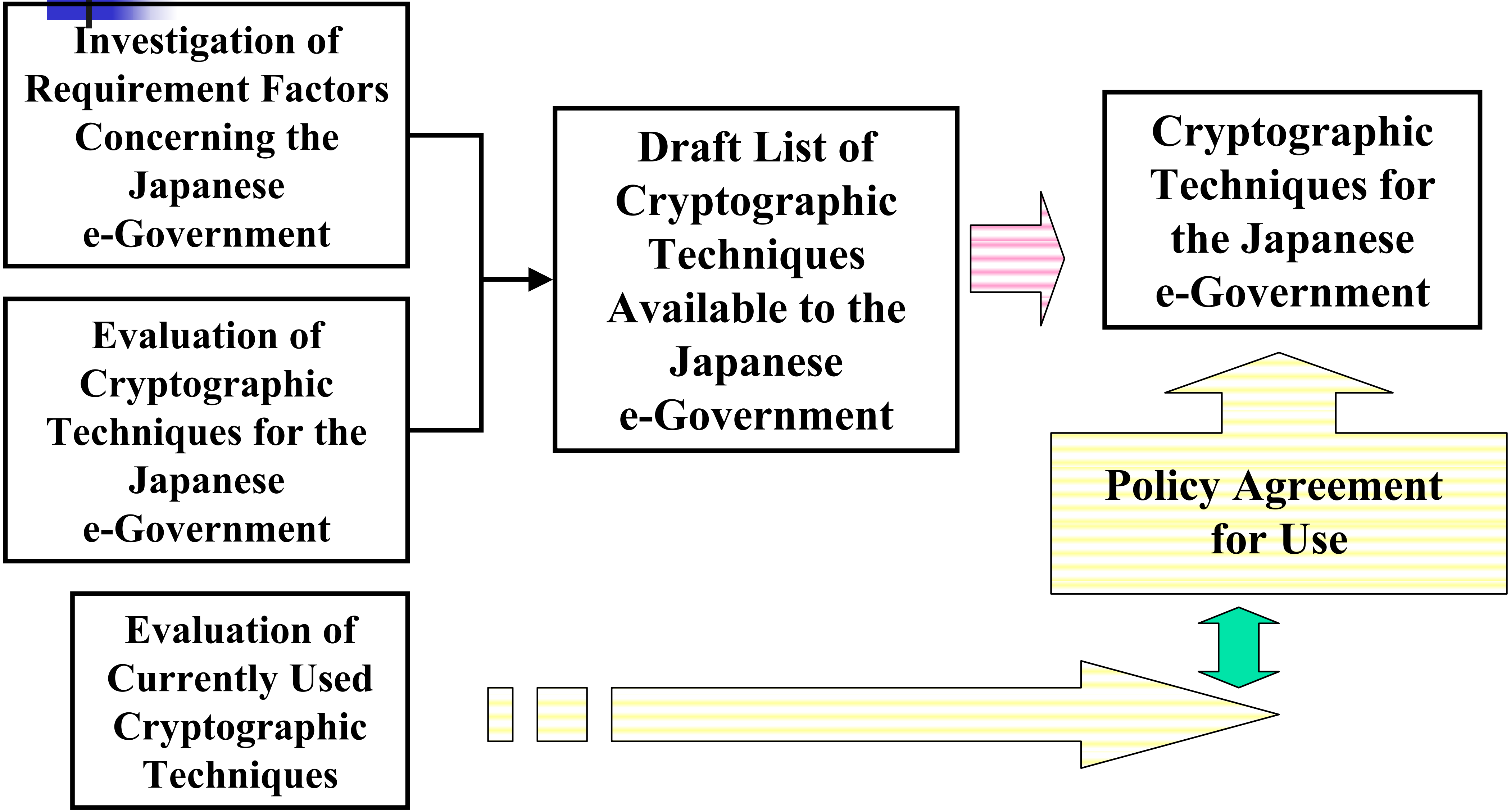
Continual Evaluation

Specific Evaluation

Cryptographic Technique Candidates for the Japanese e-Government

Cryptographic Techniques for Specific Areas

Image of Selecting Cryptographic Techniques for the Japanese e-Government



Investigation of Requirement Factors Concerning the Japanese e-Government

Evaluation of Cryptographic Techniques for the Japanese e-Government

Evaluation of Currently Used Cryptographic Techniques

Draft List of Cryptographic Techniques Available to the Japanese e-Government

Cryptographic Techniques for the Japanese e-Government

Policy Agreement for Use

Future Works

- Evaluating cryptographic techniques indispensable for the Japanese e-Government in FY 2003
- Effective use of CRYPTREC evaluation results
- Works in cooperation with other organizations such as
  - NESSIE
  - AES
  - ISO/IEC
- Continual evaluation by a public and neutral organization

Schedule

October 9-10, 2001: Cryptographic Technique
Submissions Briefing

January, 2002: Cryptographic Techniques
Evaluation Workshop

March, 2002: CRYPTREC Report 2001