Role of Cryptographic Evaluations in e-Japan Strategy

January 28, 2002

Hidetoshi Ono, Director, Office of IT Security Policy, Ministry of Economy, Trade and Industry

CRYPTREC Advisory Committee
(Chair: Hideki Imai, Professor, University of Tokyo)

In order to establish usage policies relating to cryptographic techniques in Japanese e-Government, Japanese cryptographers have been assembled to evaluate ciphers from specialized perspectives (IPA and TAO are the evaluation offices) as a joint project of the Ministry of Economy, Trade, and Industry and the Ministry of Public Management, Home Affairs, Posts and Telecommunications (formerly the Ministry of Posts and Telecommunications). The Cabinet Secretariat, the National Police Agency, the Defense Agency, the Ministry of Justice, the Ministry of Finance, and the Ministry of Foreign Affairs have all collaborated on this. The meeting of the Committee will be held by the coordinating bureau heads of both ministries.

Subjects	**:**	**Symmetric-key ciphers (block, stream), asymmetric-key ciphers, hash, etc.**
Evaluation criteria	**:**	**Security, flexibility, efficiency, and other features related to cryptographic algorithms**
Call method	**:**	**Call for candidates to provide broad, transparent acceptance of proposals (also accepted from foreign countries)**

(in addition, other ciphers will also be evaluated)

Activities of CRYPTREC Advisory Committee

1. Listing the ciphers recommended for e-government

A list of recommended ciphers relating to cryptographic algorithms used by electronic application systems and other e-government systems will be created to contribute to the development of highly secure and reliable systems. As part of this effort and as a continuation of last year's activities, follow-up evaluations and new evaluations will be conducted, and a study relating to cipher requirements for e-government will be conducted by a working group (led by Professor Sasaki of Tokyo Denki University).

2. Advice for ciphers to be used based on Electronic Signature Law

(1) Impact of Electronic Signature Law, Article 2, Clause 3 on electronic signature criteria (relating to cipher); and review

(2) Research on evaluations of cryptographic techniques based on Electronic Signature Law, Article 33

3. Support for international standardization related to cryptographic techniques

The committee will provide support for activities relating to the international standardization of ciphers in forums such as ISO and ITU.

Role in e-Japan Priority Policy Program (March 29, 2001, IT Strategic HQ)

6. Ensuring security and reliability of advanced information and telecommunication networks

(3) Specific measures

1. Establishment of system and platform for information security

c) Standardization of cryptographic techniques (Ministry of Public Management, Home Affairs, Posts and Telecommunications and Ministry of Economy, Trade, and Industry)

In order to adopt cryptographic techniques with superior performance whose security has been objectively evaluated, by FY2002 we will evaluate and standardize cryptographic techniques that will be helpful in e-government applications and the like. This will be accomplished by holding advisory committee meetings and the like involving experts, in consideration of international standardization of cryptographic techniques by organizations such as ISO and ITU.

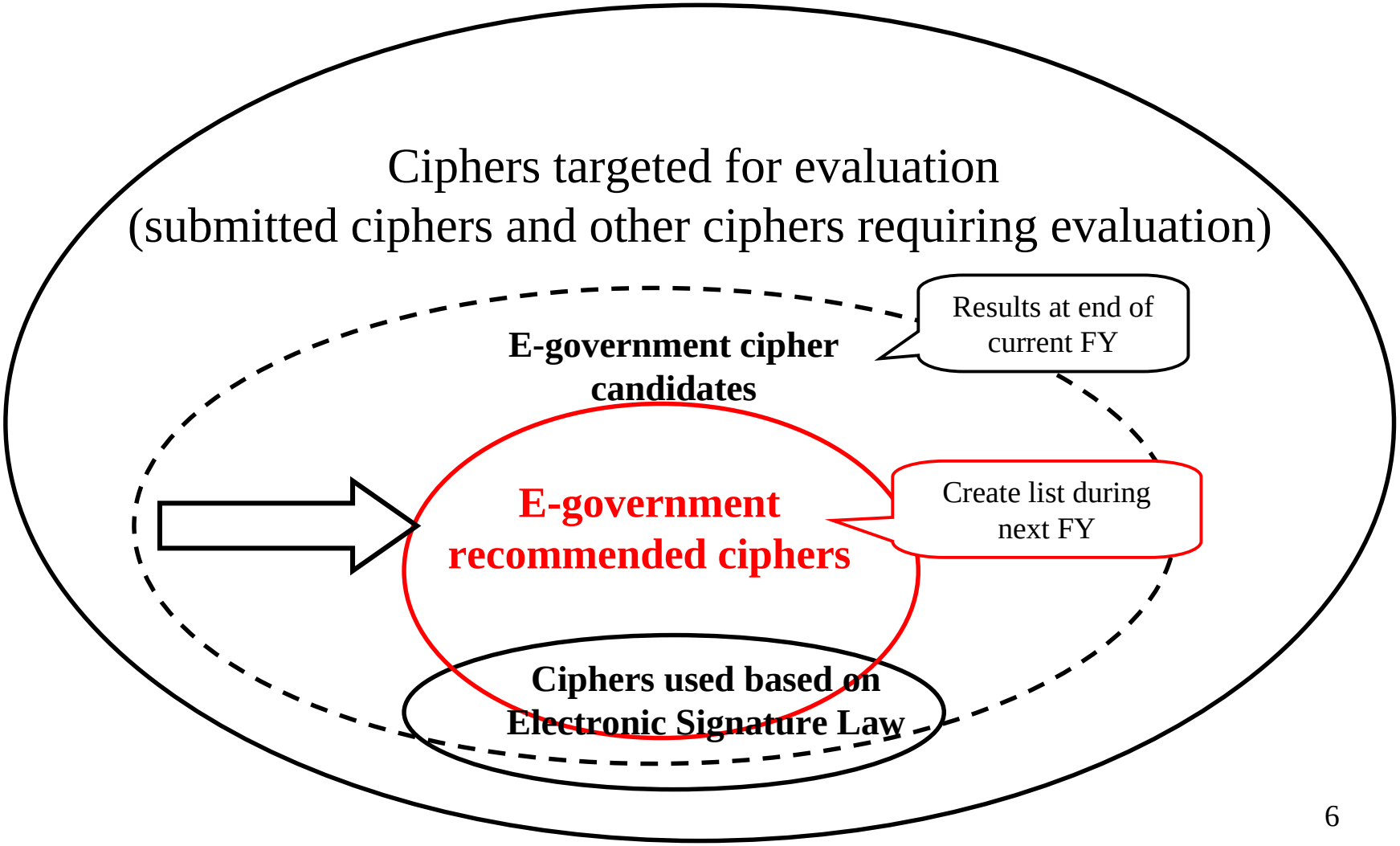
Action plan for ensuring e-government information security (October 10, 2001 Decisions made at information security measures meeting)

2. Specific measures

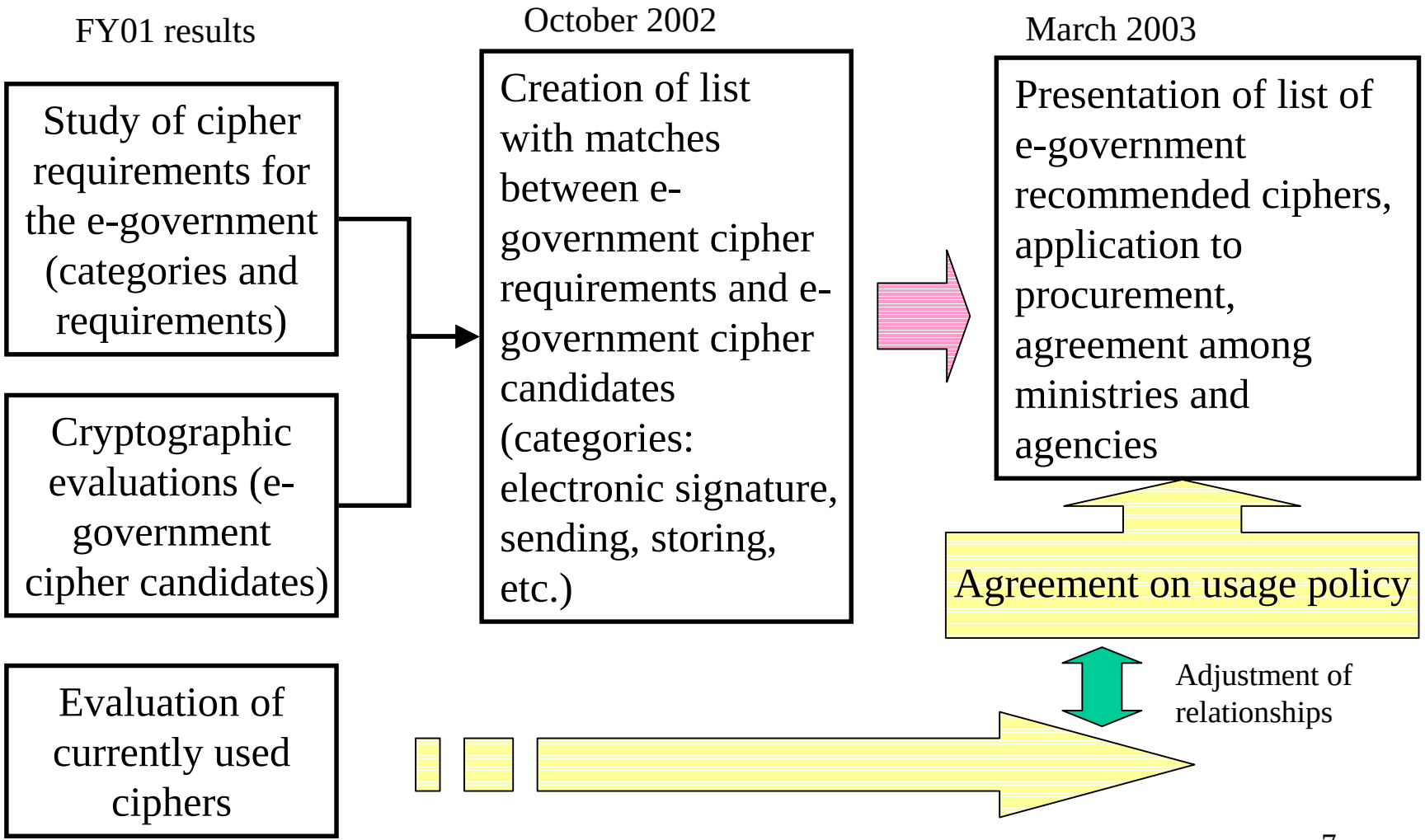
(2) Cipher standardization

- In order to ensure security for “e-government”, to the extent possible we will use criteria (specifically, ISO/IEC 15408) pertaining to information equipment and the like designed to provide a specific level of security for government procurement. In the same manner, it is essential to use and promote ciphers providing at least a specific level of security and reliability.
- To this end, the *Ministry of Public Management, Home Affairs, Posts and Telecommunications and Ministry of Economy, Trade, and Industry will create a list of ciphers recommended for the Japanese e-Government procurement in FY2002, taking into consideration data such as the results of a research committee run by these ministries. Based on these findings, our goal is to reach an agreement among ministries and agencies regarding cipher usage policy.*

E-government recommended ciphers



Future plan


FY01 results
October 2002
March 2003
Study of cipher requirements for the e-government (categories and requirements)
Cryptographic evaluations (e-government cipher candidates)
Evaluation of currently used ciphers
Creation of list with matches between e-government cipher requirements and e-government cipher candidates (categories: electronic signature, sending, storing, etc.)
Presentation of list of e-government recommended ciphers, application to procurement, agreement among ministries and agencies
Agreement on usage policy
Adjustment of relationships

Overview of usage policy draft

Usage policy level

…(omitted)…
In developing information systems in the future, in order to ensure high security reliability, each ministry or agency shall use cryptographic techniques such as those provided in the attachments to the extent possible.

Attachments

	Cryptographic techniques	(Requirements)
Electronic signature	Cipher A, Cipher B	Security, performance, etc.
Communication	Cipher C, Cipher D, Cipher E	Security, performance, etc.
Storing	Cipher F, Cipher G	Security, performance, etc.
Other	Cipher H, Cipher I	Security, performance, etc.

Plus procurement guidebook

(An explanatory guidebook for procurement personnel for use in actual applications.)