



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

TOPICS

Report from Study Group on Enforcement of the Law Concerning Electronic Signatures and Certification Services

Introduction

MIC, the Ministry of Justice (MOJ) and the Ministry of Economy, Trade and Industry (METI) set up the Study Group on Enforcement of the Law Concerning Electronic Signatures and Certification Services (Chair: Ph.D. TSUJII Shigeo, President of Institute of Information Security) in December 2007 in order to investigate the enforcement of laws concerning electronic signatures and certification services (referred to below as the electronic signatures law).

The study group compiled and announced its investigation findings in May 2008 in the Report from Study Group on Enforcement of the Law Concerning Electronic Signatures and Certification Services. The outline of this report is introduced here.

Outline and state of enforcement of electronic signatures law

(1) Outline of electronic signatures law

(a) Goal of electronic signatures law

The electronic signatures law gives a legal definition to electronic signatures, thereby working to promote distribution and information processing through

electronic information by the smooth use of electromagnetic signatures, and through this contributes to the improvement of people's lives and the healthy development of the popular economy (article 1). It was issued in May 2000 and came into effect on April 1, 2001.

(b) Definition and conditions of electronic signatures and certification services

The electronic signature is a measure that is implemented for information that is recorded electromagnetically, and exists in order to show that a particular piece of information was created by the person who performed the measure. In addition, it enables certification that no changes have been made to that particular piece of information (article 2-1).

Also, the electronic signature system defines the following 3 duties for certification services. More specifically, "certification services" is the business that certifies that the information that is needed to verify who is the person who has used the electronic signature for the person who receives the information on which the electronic signature has been applied concerns the user (article 2-2). Within these certification

CONTENTS

■ ■ ■

TOPICS

Report from Study Group on Enforcement of the Law Concerning Electronic Signatures and Certification Services

..... 1

■ ■ ■

**International Policy Division,
Global ICT Strategy Bureau
Ministry of Internal Affairs and
Communications (MIC)**
1-2, Kasumigaseki 2-chome, Chiyoda-ku, Tokyo 100-8926, Japan
Fax: +81-3-5253-5924
Tel: +81-3-5253-5920

We welcome your comments via:
http://www.soumu.go.jp/joho_tsusin/eng/contact.html

MIC Communications News is available at:
http://www.soumu.go.jp/joho_tsusin/eng/newsletter.html

Presentation materials of MIC are available at:
http://www.soumu.go.jp/joho_tsusin/eng/presentation.html

E-mail distribution of this newsletter is possible if desired.

services, the certification services that are performed with regard to electronic signatures that conform to the standards prescribed by the ordinance of the related ministries are shown as "designated certification services" (article 2-3). Furthermore, among these designated certification services, the certification services that have received accreditation as having fulfilled the standards related to methods of installation or business will be known as "accredited certification services" (Enforcement

Regulations (*1) Article 6-2)

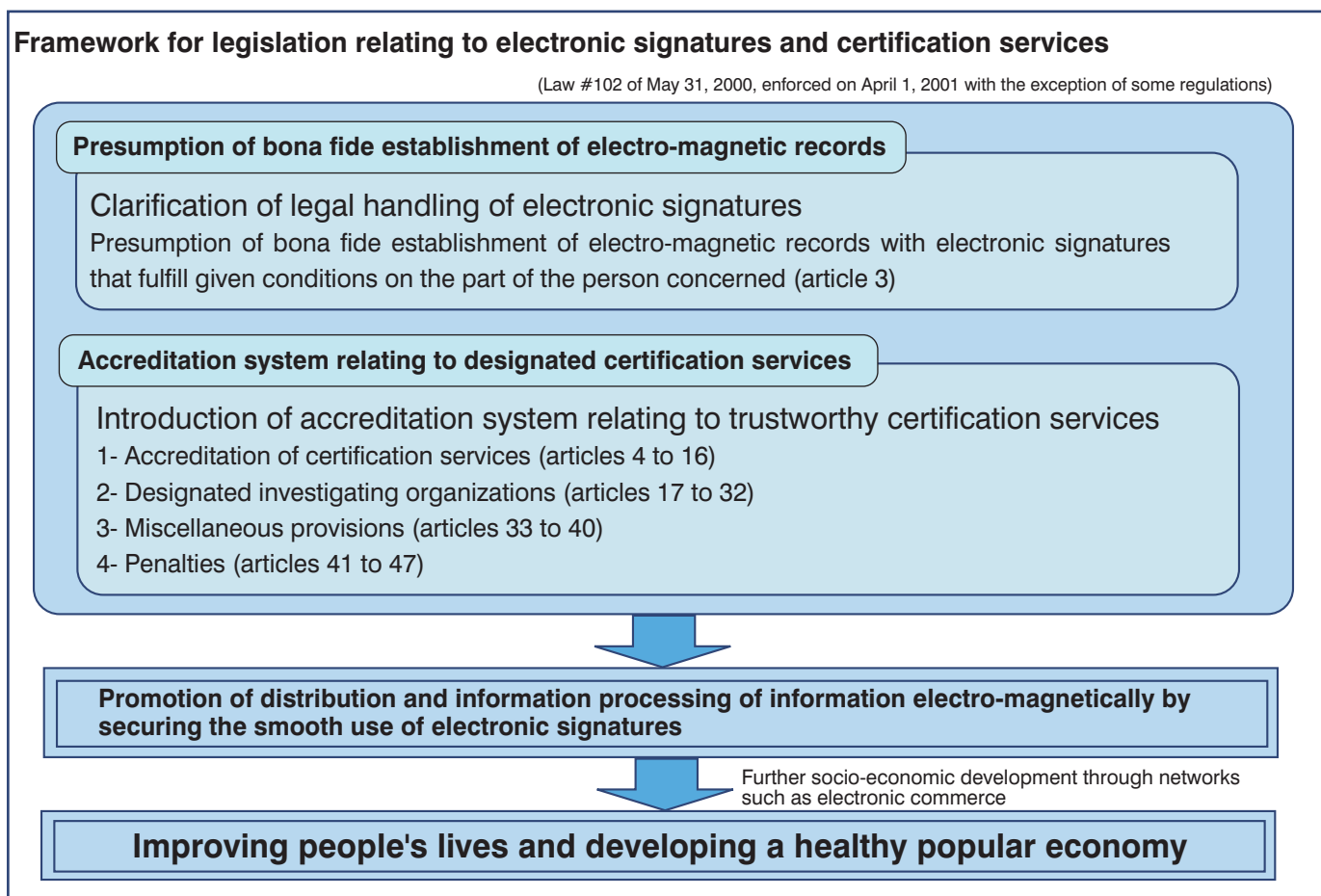
(c) The framework of the electronic signatures law

The electronic signatures law is based on two sets of regulations.

The first is that the information recorded on an electro-magnetic record shall be presumed to be authentic if an electronic signature is performed by the principal in relation to information recorded in the electro-magnetic record. (complies with article 228-4 of the Code of Civil Procedure) (article 3).

Another is the regulation that people performing designated certification services may receive accreditation from the relevant ministers (article 4), in the expectation that this will make it easier to apply in the courts the above projected regulations regarding electronic signatures for accredited certification business, putting in place a system that will be a standard for the trustworthiness of certification services as far as the people are concerned (Figure 1).

Figure 1



(2) The state of enforcement of the electronic signatures law

The number of electronic certificates relating to accredited certification services is increasing year by year. As of the end of fiscal year 2006, an accumulated total of 310,000 certificates had been

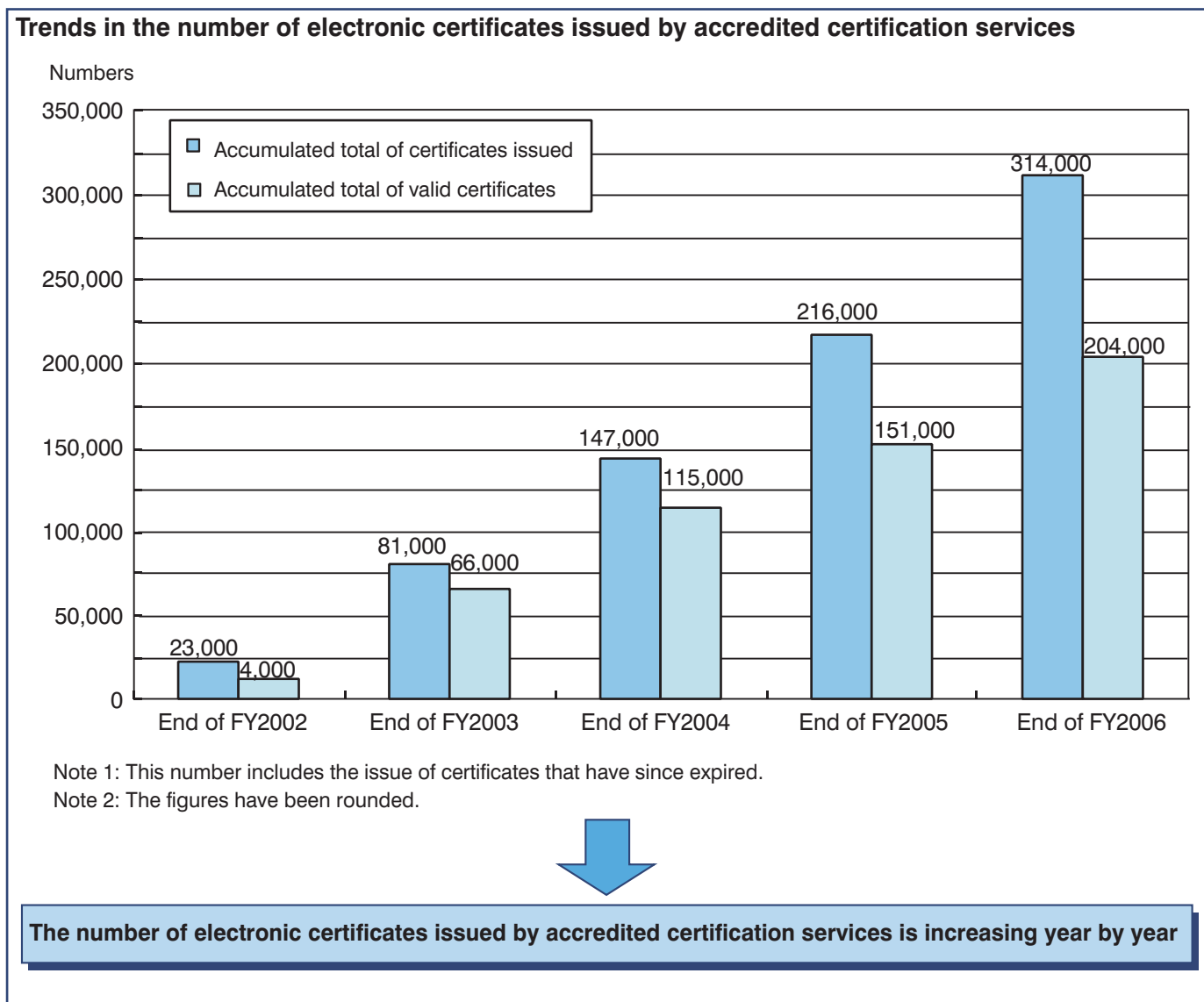
issued (about 200,000 valid ones) (Figure 2).

In addition, the number of accredited certification service operators stood at 10 companies at the end of fiscal year 2002, almost doubling to 18 companies by the end of fiscal year 2003, and

continuing to evolve steadily since then.

The main applications for the electronic certificates issued by these accredited certification service operators are electronic applications, electronic tenders and electronic contracts.

Figure 2



Results of study group's investigations

The following introduces the main questions tackled by the study group, as well as the results of its investigations.

(1) On measures relating to the improvement in the safety of the encryption technology used in electronic signatures (technical question)

(a) Question

Of the encryption that is stipulated at present in the electronic signatures law enforcement regulations and notices, a drop in

safety has been pointed out in the SHA-1 hash functions and the RSA 1024 bit encryption key. So, what type of technology should be adopted in the future?

(b) Result of investigations

Looking ahead to the discontinuation of new electronic signatures using SHA-1 and RSA1024 bit, based on the electronic signatures relating to the designated certification services regulated in article 3 of the guidelines (*2), and to encourage the shift to encryption technology that offers greater safety, it would

be appropriate to move rapidly to SHA-2 (SHA-256, SHA-384, SHA-512), and to include certification services for electronic signatures with SHA-2 and RSA-2048 bit in designated certification services.

The principal ministries should proceed with the work of revising the system, based on the schedule in figure 3. Also, taking into consideration the opinion of the Study Group on Encryption Technology, a contingency plan should be put in place rapidly to deal with any sudden threats to encryptions.

Figure 3

Early part of fiscal year 2008	Start of concrete investigations with the aim of a shift in encryption algorithms, with the addition of SHA-2 to the standards for electronic signatures relating to designated certification services
(Fiscal year 2010)	(Start of encryption shift in government organization systems) * according to guidelines for shift of government organization systems (*3)
(Fiscal year 2013)	Completion of formulation of environment to handle new and old encryption algorithms within government organization systems (SHA-1, SHA-2, RSA 1024 bit and 2048 bit) * according to guidelines for shift of government organization systems
By end of fiscal year 2013	Implementation where necessary of investigation with regard to accredited certification service operators of changed accreditation relating to encryption shifts, and, on the part of accredited certification service operators, in cases where there is a need to create new key pairs for the originator using RSA 2048 bit, doing so.
By early 2014	Accredited certification services start to operate certification services with regard to electronic signatures using SHA-2 and RSA 2048 bit, activating with originator key pairs using RSA 2048 bit.
Target of around the end of fiscal year 2014	Following the validity period of user electronic certificates with SHA-1 or RSA 1024 bit, the elimination of SHA-1 and RSA 1024 bit from the standards of electronic signatures related to designated certification services. (With regard to the validity period of user electronic certificates with SHA-1 or RSA 1024 bit, each accredited certification business is requested to plan ahead, taking into consideration the shift to user electronic certificates with SHA-2 and RSA 2048 bit)

(2) Concerning the authentication of users in accredited certification services (systemic question)

(a) Question

With regard to the verification of the authenticity of users when issuing an electronic certificate as part of an accredited certification service, would it not be possible to recognize an alternative verification method for authentication, in addition to current methods (certification through a photocopy of a resident card or the like)?

(b) Result of investigations

With regard to documentation through which it is possible to check information on user name, address and date of birth, if the same level of verification of authentication of the user as is currently used is maintained, and a certain reliability in laying down in the law the reasoning behind the making of these documents is

recognized, a revision of enforcement regulations that the presentation of these documents can replace the presentation of necessary documents should be given full consideration.

With regard to the 4 professional organizations (*4) that are accredited certification service operators, they manage the registers of names based on the various laws governing professional organizations, but if the legislation that forms the basis of these registers and the actual conditions of operating and managing them are to be in line with the purpose of the electronic signatures law, it is conceivable that it would be possible to recognize, in certain cases, as a method that would replace the presentation of necessary documents. It is necessary for the relevant ministries to continue their investigations with the aim of revising the enforcement regulations in the course of fiscal

year 2008.

(3) Concerning measures for promoting penetration (business question)

(a) Question

Is it not necessary for the government, as per the gist of articles 33 and 34 of the electronic signatures law, to make efforts to spread electronic signatures offering assistance to designated certification service operators and their users, conducting ongoing PR activities concerning electronic signatures, and, if necessary, investigating other measures?

(b) Result of investigation

The investigation and implementation of the following penetration promotion measures would be appropriate. With regard to concrete contents, investigations should be conducted centering on the three ministries most concerned.

- Ongoing implementation of penetration promotion measures that have been conducted to date, based on articles 33 and 34 of the electronic signatures law.
- Coordination with public individual certification services (usage of public individual certification services as providers of trust anchors that secure the physical verification needed by accredited certification service operators).

Conclusion

MIC, together with MOJ and METI, will take this report into consideration and conduct further investigations ahead of the shift in encryption algorithms, promote of the penetration of electronic

signatures, and by working to coordinate with related organizations put together the necessary measures to contribute to the smooth operation of the electronic signature law, thus putting in place a safe and secure network usage environment, and working for the promotion of greater socio-economic activity using networks, starting with e-commerce and e-government.

(*1) "Regulations for the Enforcement of the Law Concerning Electronic Signatures and Certification Services." (2001 MIC, MOJ, METI ministerial ordinance #2)

(*2) "Guidelines relating to accreditation of designated certification

services based on the Law Concerning Electronic Signatures and Certification Services" (2001 MIC, MOJ, METI ministerial ordinance #2)

(*3) Guidelines for the shift of SHA-1 and RSA 1024 encryption algorithms used in the information systems of government organizations (April 22, 2008, Information Security Policy Conference)

(*4) The four organizations are: Japan Federation of Certified Public Tax Accountants' Associations, Japan Federation of Land and House Investigators' Associations, Japan Federation of Solicitor Associations, and All Japan Federation of Certified Social Insurance and Labour Consultant Associations