Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline

Chapter 1 General

Article 1 (Purpose) This Guideline aims to provide for matters that require compliance by certificate authority and registration authority ("Certificate Authorities" hereinafter) as they identify an applicant before issuing web server security, code-signing and secure e-mail certificates ("Certificates" hereinafter).

Article 2 (Definitions) ① The terms used herein shall have the following meanings:

1. "Web server security certificate" refers to a certificate used to form trust between subscriber and web server by authenticating the existence of online transaction party via SSL (Secure Socket Layer) and to create secure channel by encrypting/decrypting data exchanged between web browser and web server.
2. "Code-signing certificate" refers to a certificate used to ensure reliability of software programs distributed on the Internet by adding digital signatures to such programs.
3. "Secure e-mail certificate" refers to a certificate used to ensure integrity, sender authentication and confidentiality of e-mail transmitted on the Internet by encrypting and adding digital signature such e-mail.
4. "Domain registration certificate" refers to a certificate issued by a national Internet registry specified in the Act on Internet Address Resources (Act No.: 7142) and stating domain name and registrant, etc.

② Except for the terms defined in Paragraph 1 above, the terms uses herein have the same meaning as defined in relevant laws and regulations.

Article 3 (Scope of Application) This Guideline is applied to identification process and procedure as web server security, code-signing and secure e-mail certificates are issued to individuals or corporations.

Chapter 2 Identification of Certificate Issuance Applicant

Article 4 (Identification for Issuance of Web Server Security Certificate) ① While identifying applicants for Web server security certificates in person, certification

authorities shall verify the following:

1. Identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act;
2. Domain registration certificate;
3. Domain registration application or registration fee payment receipt.

② Certificate authorities shall verify the validity of domain stated in the domain registration certificate of Paragraph 1 Sub-Paragraph 2 above via domain information search service. If the domain registrant name does not match the real name of certificate issuance applicant, certificate authorities shall verify the agreement document on domain use containing the signature of domain owner and the identification certificate of domain owner as in Paragraph 1 Sub-Paragraph 1 above to confirm license to use domain in issue.

Article 5 (Identification for Issuance of Code-Signing Certificate) ① While identifying applicants for code-signing certificates in person, certification authorities shall verify the following:

1. Identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act;
2. Domain registration certificate.

② Certificate authorities shall verify the validity of domain stated in the domain registration certificate of Paragraph 1 Sub-Paragraph 2 above via domain information search service.

Article 6 (Identification for Issuance of Secure E-mail Certificate) ① While identifying applicants for secure e-mail certificates, certification authorities shall verify the following:

1. Identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act;
2. E-mail address.

② Certificate authorities shall verify the validity of e-mail address in Paragraph 1 Sub-Paragraph 2 above.

Chapter 3 Verification of Online Certificate Issuance Application Information

Article 7 (Identification over Communication Network) ① If receiving the information in Article 4 to 6 online, certificate authorities shall verify the following information in addition:

1. In case of individual
   A. Telephone number under the name of applicant;
   B. Copy of identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act.

2. In case of corporation or organization
   A. Representative telephone number;
   B. Service administrator name and telephone number;
   C. Copy of identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act.

② Certificate authorities shall verify the phone number of certificate issuance applicant in Paragraph 1 Sub-Paragraph 1 and 2 in the above with a 3rd party telephone number information service agency to confirm if the owner of telephone number is the same person as certificate issuance applicant.

③ Certificate authorities shall verify the reliability of certificate issuance application information with certificate issuance applicant and service administrator over the phone and reject online certificate issuance application and conduct in-person verification if they are not accessible by the phone.

Chapter 4 Renewal, Modification, Re-Issuance of Certificate

Article 8 (Renewal, Modification, Re-Issuance of Certificate) ① In renewing, modifying or re-issuing certificates of certificate issuance applicants, certificate authorities shall comply with the identification procedures stipulated in Article 4 to 7 herein.
② In case of certificate renewal as in Paragraph 1 above, certificate authorities may identify applicable existing subscriber by digital signature.
③ In case of web server security certificate renewal, certificate authorities shall verify the validity of domain specified in such certificate in addition to the provision in Paragraph 2 above.