Communiqué on Processes and Technical Criteria Regarding Electronic Signatures

PART ONE
General Provisions

Purpose

Article 1 – The purpose of this Communiqué is to set out detailed processes and technical criteria related to electronic signatures.

Scope

Article 2 – This Communiqué covers technical details regarding ECSP operations including application for qualified electronic certificate generation, dissemination, renewal, revocation of certificates and archiving process, signature creation and verification data, certificate policy and certification practice statement, secure signature creation and verification devices, system, device and physical security used in the operations of ECSP, ECSP's staff, time-stamp and its services.

Legal Basis

Article 3 – This Communiqué is prepared in accordance with the Article 34 of the Ordinance Regarding the Procedures and the Rules Pertaining to the Implementation of Electronic Signature Law.

Definitions

Article 4 – The definitions used in this Communiqué have the following meanings;

Ordinance: Ordinance Regarding the Procedures and the Rules Pertaining to the Implementation of Electronic Signature Law

BS : British Standards,

CEN : Comité Européen de Normalisation,

CWA : CEN Workshop Agreement,

DSA : Digital Signature Algorithm,

ECDSA : Elliptical Curve DSA,

EAL : Evaluation Assurance Level,

ETSI : European Telecommunications Standards Institute,

ETSI SR : ETSI Special Report,

ETSI TS : ETSI Technical Specification,

FIPS PUB : Federal Information Processing Standards Publications,

IETF RFC : Internet Engineering Task Force Request for Comments,

ISO/IEC : International Organization for Standardization / International Electrotechnical Committee,

ITU : International Telecommunications Union,

RIPEMD : RACE Integrity Primitives Evaluation Message Digest,

RSA : Rivest-Shamir-Adleman,

SHA : Secure Hash Algorithm

Moreover, for the terms not defined but used in this Communiqué, the definitions in the Law and Ordinance shall apply.

PART TWO
Technical Issues

ECSP Operations

Article 5 – ECSP shall ad pt the following standards to its all operational phases;

a) ETSI TS 101 456 and
b) CWA 14167-1

Qualified electronic certificates shall be generated in conformity with the following documents;

a) ETSI TS 101 862 and
b) ITU-T Rec. X.509 V.3

Algorithms and Parameters

Article 6 – Signature creation and verification data shall be generated in conformity with following algorithms and parameters;

a) Signature creation and verification data of signature owner's
   i. ≥1024 bits for RSA or
   ii. ≥1024 bits for DSA or
   iii. ≥160 bits for ECDSA
b) Signature creation and verification data of ECSP
   i. ≥2048 bits for RSA or
   ii. ≥2048 bits for DSA or
   iii. ≥256 bits for ECDSA

Following algorithms shall be used for hashing;

a) RIPEMD – 160 or
b) SHA – 1

The algorithms and parameters stated above will be valid until 31/12/2005.

Algorithms and parameters in ETSI SR 002 176 should be used provided that they comply with the algorithms and parameters above.

Certificate Policy and Certification Practice Statement

Article 7 – ECSP shall prepare CP and CPS conformant to IETF RFC 3647.

Secure Signature Creation and Verification Devices

Article 8 – Secure signature creation devices shall be conformant to CWA 14169 or assured to EAL4+ in accordance to ISO/IEC 15408 (-1,-2,-3).

Secure Signature Verification Devices (SSVD) supplied by an ECSP shall be conformant to CWA 14171 and ECSP shall also make a declaration of conformity for these SSVDs.

Security Criteria

Article 9 – ECSP shall ad pt following standards for its security;

a) CWA 14167-1,
b) ETSI TS 101 456 and

c) ISO/IEC 17799

Time-stamp and Time-stamping Services

Article 10 – ECSP shall meet the following requirements regarding time-stamps and time-stamping services;

a) CWA 14167-1 and
b) ETSI TS 101 861

Time-stamp policy and time-stamping practice statement shall be prepared conformant to ETSI TS 102 023.

Documents

Article 11 –

a) ECSP shall be awarded the certificate BS 7799-2,
b) ECSP shall have certificates, obtained from the authorized institutions or organizations, for its Secure Signature Creation Devices either;
    i. Meet the requirements identified in FIPS PUB 140-1 or FIPS PUB 140-2 level 3 or higher, or
    ii. Meet the requirements identified in CWA 14167-2, or
    iii. Meet the requirements identified in CWA 14169 or assured to EAL4+ or higher in accordance to ISO/IEC 15408 (-1,-2,-3).

PART THREE
Miscellaneous Provisions

Entry into Force

Article 12 – This Communiqué shall enter into force on the date of its publication.

Execution

Article 13 – The provisions of this Communiqué shall be executed by the Chairman of the Board.