A Proposal of ESIGN-PSS to IEEE P1363

NTT Information Sharing Platform Laboratories
Nippon Telegraph and Telephone Corporation

August 24, 2006

1 Proposal

The IEEE P1363 document states, in its description of IFSSA signature scheme, as follows (Section 10.3.1 c) 3), p.53):

> **3) If the signature primitive is IFSP-ESIGN, then the message-encoding should be EMSA5 or a technique designated for use with IFSSA and this signature primitive in an amendment to this standard.**

We propose to update the above statement as follows:

> **3) If the signature primitive is IFSP-ESIGN, then the message-encoding should be EMSA4, EMSA5 or a technique designated for use with IFSSA and this signature primitive in an amendment to this standard.**

2 Rationale

2.1 ISO/IEC 14888-2

The current draft of ISO/IEC 14888-2 (2nd FCD) has been updated so that the use of PSS (EMSA4) is now recommended as a formatting mechanism (i.e., message-encoding) combined with several signature primitives, including ESIGN [1].

2.2 Security of ESIGN-PSS

The security of ESIGN primitive combined with PSS (EMSA4) is already evaluated [2], and it is shown to satisfy a stronger security requirement (i.e., existential unforgeability against adaptive chosen-message attacks), as compared to the one with TSH (EMSA5).

2.3 Performance

The performance of ESIGN-PSS is about the same as that of TSH-ESIGN.

3 Patent information

NTT grants non-exclusive, royalty-free licenses of the essential patents for ESIGN.

References

[1] *ISO/IEC 14888-2, 2nd FCD, Information technology — Security techniques — Digital signatures with appendix — Part2: Integer factorization based mechanisms.* June 30, 2006.

[2] T. Kobayashi and E. Fujisaki, "Security of ESIGN-PSS," Submission to *IEICE Transaction of Fundamentals of electronic Communications and Computer Science.*