F.No.CCA/DC(T)/2013-98 (pt.)
Government of India
Ministry of Communications & Information Technology
Department of Electronics & Information Technology
Office of Controller of Certifying Authorities
New Delhi

25th October 2013

OFFICE ORDER

The Security of Private keys corresponding to the DSCs being issued by Certifying Authorities (CA) to subscribers has always been a matter of concern. In this regard, the Certificate Policy pertaining to India PKI lays down the technical security controls for key pair generation and installation (Section 6 of India PKI CP Version 1.1). Detailed instructions were also issued on vide our letter No. 13(2)/2009-CCA dated 23rd September 2009 covering guidelines for storage of Private Keys, and the same has been reemphasized subsequently in meetings held with the CAs (ref. minutes of meeting held with all CAs on 19th October 2012 and 23rd January 2013). The compliance to this requirement is however not entirely satisfactory and it is imperative that procedures are put in place to ensure that no Class 2 or Class 3 DSCs are issued in cases where the key pair has not been generated on a FIPS 140-1/2 Level 2 validated Hardware Cryptographic Token.

CAs are advised to ensure that procedures to give effect to the above are immediately incorporated in the DSC issuance process (if not done yet) so that the Security of Private Keys used by subscribers is maintained.

In respect of Class 1 Certificate, in case the subscriber does not wish to procure a Cryptographic device, the corresponding risk should be made known to the subscriber and an undertaking taken from him/her to the effect that he/she is aware of the risks associated with storing private key(s) on a device other than a FIPS 140-1/2 validated cryptographic module.

A compliance to this should be reported to the Office of CCA within a month. This is being incorporated in the audit process.

Debjani Nag

(Debjani Nag)
Deputy Controller (Technology)