NEW DIGITAL SIGNATURE CERTIFICATE VALIDITY PERIOD

Office of the Controller of Certifying Authorities

Ministry of Communications and Information Technology

Government of India

Electronics Niketan

6, CGO Complex, New Delhi – 110 003

Dated 18.03.2011

Implementation of Interoperability Guidelines Version 2.1

1. From January 1, 2012 **only** SHA-256 Hash Algorithm and 2048 bit RSA Key Digital Signature Certificates will be issued.

2. However, from 4th April 2011, Certifying Authorities should issue Digital Signature Certificates with SHA-256 Hash Algorithm & 2048 bit RSA Key, to any applicant who requests for the same.

3. All other Digital Signature Certificates issued during 4th April 2011 to 31st December 2011 will have a validity period of one year only.

4. All other stipulations made in the Interoperability Guidelines must be adhered to.