

**Advisory Note to Relying Parties**

**30<sup>th</sup> December 2011**

All persons or organizations (Relying Parties) relying on Digital Signature Certificates issued by TCS Certifying Authority under the provisions of under The Information Technology Act 2000 (21 of 2000) as amended by The Information Technology (Amendment) Act, 2008 (10 of 2009) (w.e.f. 27-10-2009) are hereby advised as below.

1. Government of India vide Gazette Notification G.S.R. 783 (E) dated 25<sup>th</sup> October 2011 requires the use of SHA-1 to be discontinued and SHA-2 to be used in its place.
2. Consequently TCS CA shall not issue any Digital Signature Certificate signed with SHA-1 w.e.f. 1<sup>st</sup> January 2012.
3. All Digital Signature Certificates that have been issued signed with SHA-1 by TCS CA to its subscribers shall continue to be valid till their expiry.
4. Subscribers are solely responsible for affixing their Digital Signature using their Private Key. Relying Parties are advised to satisfy themselves that any software or application which has been used in order to affix a Digital Signature is compliant with the provisions of the abovementioned Gazette Notification G.S.R. 783 (E). TCS CA has no role in affixing Digital Signatures of any subscriber and accepts no responsibility or liability of any kind for the same.
5. Government of India vide Gazette Notification G.S.R. 782 (E) dated 25<sup>th</sup> October 2011 prescribes the procedure to be used while relying upon Digital Signature Certificates. Relying Parties are advised to satisfy themselves that any software or application that is being used to verify Digital Signatures is compliant with the provisions of G.S.R. 782 (E) and G.S.R. 783 (E).



Dr. Sundeep Oberoi

TCS Certifying Authority