

S-63 DIGITAL CERTIFICATES NOTES

Digital Certificates are files that bind a specific **public key** together with other information, to an individual or organisation. The S-63 standard uses a 2-level chain of certificates to operate the data protection scheme.

The IHB operates as the **Scheme Administrator (SA)** and has issued the root Digital Certificate for use within the protection scheme. The SA certificate used by IHO Secretariat is a self-signed certificate. It is available both as a X-509 compliant file IHO.CRT and as a text file (Scheme Administrator Public Key.txt). **Both files are contained in an SA Certificate compressed file that can be downloaded [HERE](#).**

The S-63 protection scheme requires the SA public key to be **installed on end user systems by all users of the protection scheme**. The installation of the SA certificate (and the public key held within) should be carried out as a separate, independent operation and should be subject to carefully controlled operating procedures.