Undertaking by Organization for HSM based Certificate Download

(To be printed on organization letter head / Office seal
To be signed by Authorized Signatory / Government Department in-charge.)

To:
IDSign CA,
Plot No:1303, Khanamet, Ayyappa Society,
Hyderabad. Telangana 500081

Sub: Declaration and Authorization for Certifying the KeyPair generated through the HSM

We hereby enclose the "Certificate Signing Request" (CSR) against the enclosed application by Applicant (Name) ____
towards ___________ Certificate. We declare and assure that,

- ✓ The CSR is originated by the key-pair generated in the Hardware Security Module (HSM) and we shall import the 'CA Reply' (.cer) to this HSM and use the certificate.
- ✓ We shall ensure all responsibilities towards securing the key/certificate, and implement all measures to avoid unauthorized access/usage of this key/certificate.
- ✓ The key in the HSM is marked as Non-exportable

Certificate Information :___________________________
(Organization Individual, Document Signer certificate, SSL Certificate)
Class:_______ (Class 2 or Class 3)

We confirm that, (i) Keys in the HSM are of single under (DSC applicant) and are in full control of the applicant.(ii) HSM is under the administrative & physical custody of Organisation and this signing key activation controls are only with the DSC applicant.(iii) Organization will submit the revocation request for DSC immediately in the event of the DSC applicant quitting or loss of Key or key compromise or being transferred from the Organisation.

Hardware Security Module Information:
Manufacturer:______
Model: FIPS 140-2
Level: ___________ (Class 2 or Class 3)
HSM Serial Number:________________

We authorize IDSign CA to certify given CSR, and issue the certificate

For the Organization,

(Seal and Signature)
Name & Designation:_________________________