DIGITALTRUST

APPLICATION FOR HIGH ASSURANCE ENTERPRISE/CORPORATE CERTIFICATES

The following information must be provided together with the request for End User certificates.

REQUESTOR INFORMATION	
NAME	
TITLE	
PHONE NUMBER	
EMAIL ADDRESS	

END USER INFORMATION	
FIRST NAME	
LAST NAME	
EMAIL ADDRESS	
ORGANISATION	
DEPARTMENT (OPTIONAL)	
PHONE NUMBER (NOT INCLUDED IN CERT)	
REPORTING MANAGER (NOT INCLUDED IN CERT)	
MANAGER EMAIL (NOT INCLUDED IN CERT)	
MANAGER PHONE NUMBER (NOT INCLUDED IN CERT)	

The following supporting documents must be submitted for High Assurance enterprise/corporate certificates

- Extract from employment record including photo
- Extract from corporate email directory showing the users email

By signing this certificate request we confirm that:

- All declarations made in relation to the information contained in the certificate are true and accurate;
- Reasonable measures will be taken to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate;
- The certificate will be used strictly in compliance with the relevant DigitalTrust certificate policy (CP/CPS) and Certificate Holder Agreement;
- The certificate will immediately be declared invalid if the certificate details are no longer correct or the private key is lost, stolen, or potentially compromised; and
- I accept the DigitalTrust Certificate Holder Agreement.

DATE	
SIGNATURE	