CERTIFICATE ADMINISTRATOR AGREEMENT

[v01-03-2015]

1. PARTIES TO THIS AGREEMENT:

1.1 e4 Strategic (Pty) Ltd ("**e4**"); and

1.2 The Entity named in the signature section to this agreement ("**the Entity**"); and

1.3 The Certificate Administrator named in the signature section to this agreement ("**Certificate Administrator**").

2. BACKGROUND:

2.1 Law Trusted Third Party Services (Pty) Ltd ("**LAWtrust**") operates two certificate authorities ("**CA**"s), namely the *LAWtrust2048 CA* and the *LAWtrust AATL CA* (collectively referred to as the "**LAWtrust CA**"), issuing digital certificates to entities and natural persons that are used for access control to information systems, encrypt and decrypt electronic communications and to digitally sign electronic documents.

2.2 In issuing *digital certificates*, LAWtrust acts in accordance with its *Certificate Policy* and *Certification Practice Statement* (collectively referred to as the "**CPS**") and has appointed e4 as a *registration authority* ("**RA**") for the purposes of authenticating the identity and verifying information to be contained in *digital certificates* to be used to access e4's information systems.

2.3 **The Entity requires access to e4's information systems; and, in order to facilitate this access, the e4 RA hereby appoints the Certificate Administrator to assist with the issuance and administration of *personal digital certificates* to the Entity's personnel.**

3. APPOINTMENT OF CERTIFICATE ADMINISTRATOR:

3.1 The Entity agrees to the appointment of the Certificate Administrator to fulfil certain administrative duties, including the authentication of the identity of the Entity's personnel who are required to be issued with *personal digital certificates* in order to access e4's information systems on behalf of the Entity.

3.2 The issuance of *personal digital certificates* requires *applicants* to meet with the Certificate Administrator for 'face-to-face' identification and authentication of their identity against the photographic image contained in the *applicant's* RSA ID document, passport or drivers licence.

3.3 **The Certificate Administrator agrees that the identities of all *applicants* for *personal digital certificates* shall be authenticated as contemplated in 3.1 and 3.2 and in accordance the applicable provisions of the LAWtrust CPS and e4 RA Charter.**

3.4 No *personal digital certificate* shall be issued by the LAWtrust CA without the application being electronically submitted to the e4 RA and the Certificate Administrator's digital certificate or handwritten signature being affixed to the application.

4. RETENTION OF INFORMATION:

The Entity agrees that it shall:

4.1 retain the original application, copies of either the identification document, passport or drivers licence against which the identity of the *applicant* was authenticated and any further documentation provided in support of the application.

4.2 securely retain the documentation referred to in 4.1 for a period of 5 (five) years from the date that the application is submitted to the e4 RA.

provide access to duly authorised representatives of e4 or LAWtrust to view the documentation retained by the Entity for audit and verification purposes, against reasonable notice, in writing (being not less than 3 (three) business days), provided to the Certificate Administrator to the email address provided by the Certificate Administrator to e4.

5. TRAINING:

The Certificate Administrator agrees to:

5.1 undergo the training provided by e4;

5.2 **act strictly in accordance with the certification procedures stipulated in the LAWtrust CPS and e4 RA Charter;**

5.3 act at the direction of the Information Security Officer appointed by e4 in any circumstances relating to the suspected loss or *compromise* of a *digital certificate* or the *digital certificate's* associated *private key*.

6. REVOCATION OF CERTIFICATE:

The Certificate Administrator shall immediately apply for the *revocation* of a *digital certificate* if:

6.1 **information contained in the *digital certificate* is found to be incorrect; or**

6.2 **the *subscriber* leaves the employ of the Entity; or**

6.3 **the *subscriber* or Certificate Administrator becomes aware of the actual or suspected loss or *compromise* of the *digital certificate*'s associated *private key*.**

7. REPLACEMENT OF CERTIFICATE ADMINISTRATOR:

7.1 In the event that the Certificate Administrator is unable to act, the Entity agrees to appoint a replacement *certificate administrator* to act in the Certificate Administrator's stead.

7.2 If the Certificate Administrator leaves the employ of the Entity, the Entity agrees to immediately notify e4 and co-operate with e4 in the appointment of a new *certificate administrator*.

7.3 A replacement *certificate administrator* is required to sign this agreement before commencing her/his duties as a *certificate administrator*.

SIGNED FOR AND ON BEHALF OF THE ENTITY:

Entity name: .....

Reg. no. .....

Signature o.b.o Entity: ..... *(who warrants that s/he is duly authorised)*

Name: .....

Capacity (partner/director) .....

Date: .....

SIGNED BY THE CERTIFICATE ADMINISTRATOR:

Signature: .....

Name: .....

ID no. .....

Date: .....