



[v24-06-2014]

Introduction to digital certificates at e4

e4 STRATEGIC (PTY) LTD

registration number 2006/027343/07

(e4)

55 Sixth Road, Hyde Park, Johannesburg

Phone 0860 340 000

email support@e4.co.za

Web www.e4.co.za

Entrust

www.entrust.com

LawTrust
information security solutions

www.lawtrust.co.za

Law
trusted electronic solutions

www.lawholdings.co.za



PURPOSE OF THIS DOCUMENT: You might not be aware that doing business on the internet (i.e. online) has its risks, especially when other persons try to pretend to be you and transact in your name, or they try to view your confidential information. Digital certificates are a recognised means of addressing some of these risks. **The purpose of this document is to:**

(i) draw to your attention the fact, nature and potential risks of transacting online; and

(ii) introduce to a lay-person (who is not necessarily familiar with digital certificates) the practices and procedures that need to be adhered to when using digital certificates to transact online with e4.



THIS DOCUMENT HAS BEEN MADE AVAILABLE FOR INFORMATION PURPOSES ONLY. Should you wish to be issued with a digital certificate then you need to print, complete, sign, and send back to e4 the following documents:

1. *Subscriber Personal Digital Certificate Application Form, and*
2. *LAWtrust Subscriber Agreement.*
3. *Copy of your ID, passport or driver's licence.*

*For any further queries or assistance please contact the e4 call centre on **0860 340 000**.*

TABLE OF CONTENTS

1	Introduction.....	4
2	LAWtrust certificate authority.....	4
3	e4 registration authority	5
4	e4 RA Charter	5
5	Purpose of issuing digital certificates.....	6
6	Personal digital certificates & entity digital certificates	6
7	Applicants and subscribers.....	7
8	Certificate administrators.....	7
9	Applying to be issued with a digital certificate	7
10	Submitting subscriber application to e4	8
11	Digital certificate duration and renewal	9
12	Revocation of a digital certificate.....	9
13	Digital certificate use for named subscriber only	9
14	Further information.....	10

1 Introduction

YOU MAY BE ASKING YOURSELF WHAT IS A DIGITAL CERTIFICATE, CERTIFICATION AUTHORITY, REGISTRATION AUTHORITY, CERTIFICATION PRACTICE STATEMENT, RA CHARTER, SUBSCRIBER OR ANY OF THE OTHER DIGITAL CERTIFICATE BUZZWORDS YOU MAY HAVE HEARD. IF SO, READ ON, ALL WILL BE REVEALED.

This document seeks to introduce to a lay-person (and who is not necessarily familiar with digital certificates) the practices and procedures required to be followed in authenticating (i.e. establishing as real or genuine):

- (i) the identity of a *subscriber*,
- (ii) the entity to which the *subscriber* is associated, and
- (iii) any other information that may be required before issuing a *digital certificate* in the name of the *subscriber* applying to be issued with a *digital certificate*.



This document is an information document and not part of the various documents that form the contracts required to support the policies and procedures that need to be in place to sustain a credible network of *digital certificate* users.

REMEMBER, IF AFTER READING THIS YOU ARE STILL CONCERNED, PLEASE DO NOT HESITATE TO CONTACT THE e4 CALL CENTRE ON 0860 340 000.

2 LAWtrust certificate authority

Law Trusted Third Party Services (Pty) Ltd (LAWtrust) (www.lawtrust.co.za), through the *certificate authority* (CA) it operates, issues *personal digital certificates* and *entity digital certificates* to *subscribers* in accordance with the provisions of its *certificate policy* and *certification practice statement* (collectively referred to as the “CPS”), which includes the Entrust, Inc. (www.entrust.com) policies and procedures.

 A **certificate authority**, such as LAWtrust, plays an important role in that it issues **digital certificates**, sets policy (as stated in its CPS) on what identification a **subscriber** must produce in order to obtain a **digital certificate**; and in order to maintain security, indicates in a **published certificate revocation list** those **digital certificates** that are no longer valid (e.g. Revoked, expired or suspended).

In terms of the CPS, LAWtrust may appoint **registration authorities** and prescribe the practices and procedures that the **registration authority** is to adhere to.

3 e4 registration authority

In terms of its CPS, LAWtrust has appointed **e4 Strategic (Pty) Ltd (e4)** to be a **registration authority (RA)**.

 A **registration authority (RA)** is an entity that:

- a. receives applications for the issuance of **digital certificates**;
- b. validates information supplied in support of a **digital certificate** application;
- c. requests a **certificate authority** to issue a **digital certificate** containing the information as validated by the **registration authority**;
- d. requests a **certificate authority** to revoke **digital certificates** issued.

4 e4 RA Charter

e4 OPERATES AS A **REGISTRATION AUTHORITY** IN ACCORDANCE WITH THE PROVISIONS OF ITS **REGISTRATION AUTHORITY CHARTER (RA CHARTER)** AND THE LAWTRUST CPS.

 **THE e4 RA CHARTER, SUBJECT TO THE PROVISIONS OF THE LAWTRUST CPS, DESCRIBES THE AUTHENTICATION, PERMISSIONS AND RESTRICTIONS OF SUBSCRIBERS WHEN USING DIGITAL CERTIFICATES IN ORDER TO ACCESS AND WORK ON e4'S INFORMATION SYSTEMS OVER THE INTERNET.**

5 Purpose of issuing digital certificates

Digital certificates, properly issued, can be used to manage access control to information systems over the internet, and for secure electronic communications (e.g. decrypting electronic rates clearance certificates issued by those municipalities that make use of e4's services).



The purpose of issuing *digital certificates* to *subscribers*, in accordance with the requirements of the LAWtrust CPS and e4 RA Charter, is to create an environment where it becomes commercially reasonable for persons to remotely transact electronically with each other, where the risks of being able to impersonate the electronic identity of a person, and/or alter the contents of an electronic communication unbeknownst to a recipient, are greatly reduced if not eliminated.

6 Personal digital certificates & entity digital certificates

A *personal digital certificate* is issued to a natural person. An *entity digital certificate* is issued to a legal person or a partnership (which are treated as legal persons for e4's purposes in terms hereof).

Entity digital certificates are typically used in e4's environment to enable a legal entity (e.g. a law firm) to receive electronic instructions (e.g. conveyancing or debt collection instructions) from those other entities (e.g. the banks) making use of e4's information system services to instruct them.

Personal digital certificates are typically used in e4's environment by employees (e.g. the conveyancer or his/her assistant) of the entity (e.g. a law firm) to, on the entity's behalf, carry the work required to be done in terms of the electronic instruction received.

e4 associates *entity digital certificates* and *personal digital certificates* by means of e4 User Numbers (LUN) in order to ascribe the work of a particular individual to a particular entity.



Therefore, when reading further, reference to an *applicant* or a *subscriber* depends on the context and refers to either a natural person (in respect of a *personal digital certificate*) or a legal entity or partnership (in respect of an *entity digital certificate*).

Reference to a *digital certificate* (or simply a *certificate*) refers to, depending on the context, either a *personal digital certificate* or an *entity digital certificate*.

7 Applicants and subscribers



A person/entity applying for the issuance/renewal of a *digital certificate* is described as an *applicant*, until such application has been approved and the *digital certificate* issued, whereupon the person or entity in whose name it has been issued/renewed is then referred to as a “*subscriber*.”

8 Certificate administrators

Processing applications for *digital certificates* commences with persons called *certificate administrators*, appointed and authorised by e4 to authenticate the identity of a *subscriber* and any other required information.

A *certificate administrator* may be either an authorised e4 employee or an employee of the entity (to whom an *entity digital certificate* has been issued) that requires additional *personal digital certificates* to be issued to other members of its staff.

The *certificate administrator* is required to enter into an agreement (Certificate Administrator Agreement) with e4 in the prescribed form. This agreement sets out the *certificate administrator's* delegated obligations to authenticate the identity of the *subscriber* before authorising the issuance by the LAWtrust CA of a *digital certificate* to that *subscriber*.



Certificate administrators must receive proper training in administering applications for *digital certificates*, authenticating *subscribers*, authorising the issuance of *digital certificates*, downloading and installing *digital certificates*, and *digital certificate* revocation.

9 Applying to be issued with a digital certificate

An *applicant* is required to:

1. complete a *digital certificate application form*, to be signed by the *certificate administrator* or an authorised representative of e4;
2. sign and agree to abide by the terms of the LAWtrust *subscriber agreement*;
3. in respect of *personal digital certificates*, present to the *certificate administrator* or the authorised representative of e4:
 - a. *digital certificate* application form;
 - b. *subscriber agreement*;
 - c. ID document, passport or drivers license.
4. in respect of *entity digital certificates*: present to the *certificate administrator* or the authorised representative of e4:
 - a. e4 order form;
 - b. *digital certificate* application form;
 - c. *subscriber agreement*;
 - d. certificate administrator *digital certificate* application form;
 - e. certificate administrator agreement;
 - f. debit order authority;
 - g. fidelity fund certificate;
 - h. cancelled cheque;
 - i. appointment to bank's panel of attorneys;
 - j. ID document of natural person making the application on entity's behalf;

(PLEASE NOTE: The above requirements are subject to change from time to time.
Please see www.lawholdings.co.za or contact the e4 call centre for further details)

After confirming the identity of the *subscriber*, the information contained in the *digital certificate* application form, the *subscriber's* signature of the *digital certificate* application form and the *subscriber agreement*, the *certificate administrator* is then required to counter sign the *digital certificate* application form.

10 Submitting subscriber application to e4

After completing the *subscriber* application process, the *certificate administrator* is required to:

1. confirm the application and authentication of the *subscriber* has been completed by affixing his/her *personal digital certificate* to the confirmation electronically communicated to the LAWtrust RA.
2. Fax or email to the LAWtrust RA copies of the signed *digital certificate application form*, the *subscriber agreement*, and the *subscriber's* supporting documentation.

11 Digital certificate duration and renewal



DIGITAL CERTIFICATES ARE VALID A PERIOD OF 1 (ONE) YEAR FROM THE DATE OF ISSUE, whereafter the *subscriber* will need to “renew” his/her/its *digital certificate* by making a renewed application to be issued with a *digital certificate*.

12 Revocation of a digital certificate

A *digital certificate* issued is required to be revoked, and will be revoked where:

1. the person to whom the *personal digital certificate* has been issued leaves the employ of the entity to which his/her *personal digital certificate* is associated; or
2. the *certificate administrator*, or the person/entity in whose name the *digital certificate* is issued, becomes aware of any inaccuracy of the information contained in the *digital certificate*, or suspects or knows of an actual compromise of the private key associated with the *digital certificate*.

13 Digital certificate use for named subscriber only



It is important that e4 is able to identify the person/entity using a *digital certificate* to gain access to e4's information systems, and further be able to accurately ascribe the work of a particular individual to a particular entity.

 IT IS THEREFORE THAT A *DIGITAL CERTIFICATE* IS ONLY ISSUED ON THE BASIS THAT ITS SUBSEQUENT USE IS AT ALL TIMES PERSONAL TO THE PERSON/ENTITY ACTUALLY NAMED IN THE *DIGITAL CERTIFICATE*.

 NO *SUBSCRIBER* MAY ALLOW OR OTHERWISE PERMIT THE USE OF HIS/HER/ITS *DIGITAL CERTIFICATE* BY ANY OTHER PERSON/ENTITY – SUCH ACTIONS NOT ONLY ARE A BREACH OF THE TERMS OF THE *SUBSCRIBER AGREEMENT*, BUT ALSO RENDER SUCH PERSON/ENTITY POTENTIALLY LIABLE FOR THE ACTIONS OF OTHERS MADE USING HIS/HER/ITS *DIGITAL CERTIFICATE*.

 ALSO, A *SUBSCRIBER* IS NOT ALLOWED TO USE ANOTHER PERSON/ENTITY'S *DIGITAL CERTIFICATE* IN ORDER TO ACCESS *e4'S INFORMATION SYSTEMS*.

14 Further information

Please see the LAWtrust CPS and the e4 RA Charter for further details.

FOR ANY FURTHER QUERIES PLEASE CONTACT e4'S CALL CENTRE ON

0860 340 000.
