Short Description of Ethiopian PKI Governance Documents

The documents described in this short paper are:

1. The Ethiopian PKI X.509 Certificate Policy
2. Ethiopian PKI National Root Certificate Authority Certificate Practices Statement (CPS)
3. Ethiopian PKI Site Preparation Guidelines
4. Ethiopian National PKI Technical Standards Guidelines, and
5. Security Guidelines for Certificate Authorities

The Ethiopian PKI X.509 Certificate Policy

This document describes the policies, procedures and technical details related to the issuance and control of certificates in the Ethiopian Public Key Infrastructure (PKI) for e-governance and e-commerce. It also describes the roles and responsibilities of the various actors involved in the processes and the management of the PKI. This policy applies to the entire trust chain down (i.e. from the Root CA all the way down to the end-entities). The document is developed based on RFC 3647 framework. The major points the document comprises are: (1) Introduction, (2) Publication and Repository Responsibilities, (3) Identification and Authentication, (4) Certificate Life-Cycle Operational Requirements, (5) Facility, Management and Operational Controls, (6) Technical Security Controls, (7) Certificate, CRL and OCSP Profiles, (8) Compliance Audit and Other Assessments, and (10)Other Business and Legal Matters

Ethiopian PKI National Root Certificate Authority Certificate Practices Statement (CPS)

A Certification Practice Statement (CPS) is a statement of the practices which the Root Certification Authority (Root CA) employs in issuing and managing certificates. The CPS describes in more detail how the Root CA implements the Ethiopian PKI X.509 Certificate Policy, and cannot contradict what is stated in the CP. The chapters contained in both the CP (states the ‘what’ part) and the CPS (states the ‘how’ part) are similar. The document is developed based on RFC 3647 framework as well.

Ethiopian PKI Site Preparation Guidelines

The guideline specifies the generic physical security tiers, site location, electromechanical and environmental monitoring capabilities, building management system and broad specifications of the requirements of the PKI site. The major sections contained in the document are: (1) Introduction, (2) Security Level, (3) Construction of Cryptographic Operation Site, and (4) Broad Specifications of System to be Installed.

Ethiopian National PKI Technical Standards Guidelines

This document is used to prevent the lack of interoperability between Digital Certificates issued by different Certificate Providers resulting in users having to obtain multiple numbers of Digital Certificates for use across different applications. The major sections the document comprised are: (1) Introduction, (2) Scope, (3) normative references, (4) Informative references, (5) Definitions and Acronyms, (6) Certificate Profile Guidelines, (7) Field Specification, (8) Reference Certificate Profiles, (9) Reference CRL Profile, (10) Application Developer Guidelines, and (11) Application Owner Guidelines.

Security Guidelines for Certificate Authorities

This document defines the security guidelines for the management, systems, and operations of certification authorities. It is intended for use by the management, security, technical and operational personnel of certificate authorities. The major sections of this document are: (1) Introduction, (2) Definitions and Acronyms, (3) Security Management, (4) Certificate Management, (5) Key Management, and (6) Systems and Operations Guidelines.