

Example Company, Inc.
Identity Management Architecture
Policy on Naming and Certificates

Status: [Approved | Draft – RFC | Final Draft – Awaiting Approval]

Date: 01APR04

1.0 Purpose

The purpose of this policy is to provide guidance about naming and certificates. This policy establishes the role of “Registrar” and assigns specific duties to that role.

2.0 Scope

This policy applies to all Example Company, Inc. projects, procurements, employees and affiliates.

3.0 Definitions

3.1 Domain and Subdomain. For purposes of this document, domain will be taken to mean any domain name registered by Example Company, Inc with an external registrar. Subdomain will be taken to mean any domain name within those domains.

3.2 Digital Certificates. Digital certificates are identity documents that use encryption and digital signature technologies to securely and reliably associate identity information with a public key. Certificates can be used to identify individuals or services. The X.509 standard describes the format for digital certificates.

4.0 References

Identity Reference Framework, Section 7.2, Directory Products

5.0 Policy

5.1 Registry. The Office of the CIO shall appoint a Registrar for all subdomains in the example.com and exampleservice.com domains. The Registrar shall establish procedures by which organizations within Example Company, Inc. can register subdomains. The registrar shall also maintain records of those subdomains.

5.2 Domain Names. The Registrar shall be responsible for maintaining all domain name assets that Example Company, Inc. owns. To facilitate this, the Registrar shall establish the process through which Example Company, Inc. organizations register domain names. Example Company, Inc employees are required to use the registrar’s procedure when registering any domain.

5.3 Unique Identifiers. Unique identifiers for people to be used for network access, email, and other purposes will be created within the example.com domain. Wherever possible, the identifier for a person should consist of the person’s first initial and last name. The Registrar shall establish appropriate alternative name patterns in the case of collisions. Generic identifiers (e.g. admin, webmaster, etc.) are to be used only where role-base identification is appropriate.

5.4 Organizational Certificates. Digital certificates that identify company services, servers and other assets shall be handled securely. The Registrar shall be responsible for establishing procedures to ensure that certificates are proactively managed to prevent unintended expiration or misuse

5.5 Individual Certificates. Individuals may have need of digital certificates that identify them from time to time. Individuals are responsible for managing their personal certificates and ensuring their security.

5.6 Certificate Authorities. The certificate practice statement of any certificate authority used for organizational or individual certificates shall be reviewed by the Office of the CIO and legal counsel prior to any contract for certificate services being issued.

5.7 Certificate Revocation Lists. Every system that uses digital certificates for authentication of users shall have an automatic method of checking the certificate revocation list of the certificate authority that issues the certificates and using the revocation information to disallow certificates that have been revoked.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Contacts

7.1 Custodian

IMA Team, Office of the CIO
imateam@example.com
801.555.1212 x563

7.2 Approval Body

Identity Management Architecture Review Board

8.0 Revision History

Version	Approval Date	Comments
1.0	01APR04	Initial version approved.