

PDAM Enhancements to Public-Key and Attribute Certificates

TITLE: Proposed Draft Amendment on Enhancements to Public-Key and Attribute Certificates

SOURCE: Collaborative ITU and ISO/IEC meeting on the Directory, London, England, February 2003

PDAM on Enhancements to Public-key and Attribute Certificates

Introduction

Note - This clause provides an introduction to this PDAM. The text in this clause is not intended for inclusion ISO/IEC 9594-8.

This PDAM provides enhancements for public key certificate and attribute certificate frameworks extensions and certificate revocation. Mechanisms have been developed that require changes to ISO/IEC 9594-8.

ISO 9594-8 Information Technology - Open systems Interconnection - The Directory: Authentication Framework

PDAM 1: Enhancements to Public-Key and Attribute Certificates

Clause 8 Public-key certificate and CRL extensions

8.1 Policy handling

8.1.5 Self-issued certificates

Replace a) with the following:

- a) as a convenient way of encoding its public key(s) that need to be communicated to, and stored as trust anchors by, its certificate users. Typically, the public key used to sign certificates (and possibly CRLs) would be made available in this way;

Replace b) with the following:

- b) for certifying additional key usages other than those covered by a) (such as time-stamping and possibly CRL signing); and

In the paragraph following list item c: replace "self-issued certificates of type a) are verified" with "self-issued certificates of type a) are self-signed certificates and are therefore verified..."

Add the following as a new paragraph and note at the end 8.1.5:

If an authority uses the same key to sign certificates and CRLs, a single self-issued certificate of type a) shall be used. If an authority uses a different key to sign CRLs than that used to sign certificates, the authority may choose to issue two self-issued certificates of type a), one for each of the keys. In this situation certificate users would need access to both self-issued certificates to establish separate trust anchors for certificates and CRLs signed by that authority. Alternatively, an authority may issue one self-issued certificate of type a) for certificate signing and one self-issued certificate of type b) for CRL signing. In this situation, certificate users use the key certified in the certificate of type a) as their single trust anchor for both certificates and CRLs signed by that authority.

Note: Other mechanisms for distributing CA public keys are outside the scope of this Specification.

[NOTE: Text from this PDAM, other than the proposed changes to section 8.1.5 has been removed.]