

STANDARDS AUSTRALIA

Amendment No. 1
 to
AS 4539.1.3—1999
Information technology—Public Key Authentication Framework (PKAF)
Part 1.3: General—X509 supported algorithms profile

REVISED TEXT

The 1999 edition of AS 4539.1.3—1999 is amended as follows; the amendment should be inserted in the appropriate place.

SUMMARY: This Amendment applies to Clause 7.3.

Published on 5 June 2000.

AMDT
No. 1
JUNE
2000

Page 8 Clause 7.3

Delete the existing clause and *replace* with the following:

7.3 DSA Signature keys

The object identifier supported by this Standard is —

ALGORITHM ::= { Dss-Params IDENTIFIED BY id-dsa }
Id-dsa OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) x9-57(10040) x9algorithm(4) 1 }

The id-dsa algorithm syntax includes optional parameters. These parameters are commonly referred to as **p**, **q**, and **g**. If the DSA algorithm parameters are absent from the **subjectPublicKeyinfo AlgorithmIdentifier** and the CA signed the subject certificate using DSA, then the certificate issuer's DSA parameters apply to the subject's DSA key. The parameters are included using the following structure:

Dss-Params ::= SEQUENCE {
p INTEGER,
q INTEGER,
g INTEGER }

The DSA public key shall be DER encoded as an INTEGER, as follows; this encoding shall be used as the contents (i.e. the value) of the **subjectPublicKey** component (BIT STRING) of the **SubjectPublicKeyinfo** data element:

DSAPublicKey ::= INTEGER

The intended application for the key shall be indicated in the key usage, or extended key usage field.

If the **keyUsage** extension is present in an end entity certificate that conveys a DSA public key, any combination of the following values may be present:

digitalSignature; and **nonRepudiation**.

If the **keyUsage** extension is present in a CA certificate which conveys a DSA public key, any combination of the following values may be present:

digitalSignature; **nonRepudiation**; **keyCertSign**; and **cRLSign**.

This page has been left intentionally blank.