http://www.w3.org/2008/xmlsec/Drafts/xmldsig-core-11/Overview.htm#sec-DSA

Security considerations regarding DSA key sizes

Per FIPS 186-3 [DSS], the DSA security parameter L is defined to be 1024, 2048 or 3072 bits and the corresponding DSA N value (bit lengths of p and q) is defined to be 160, 224and 256 bits respectively. Special Publication SP 800-57 Part 1 [SP800-57], NIST recommends using at least at 2048-bit public keys for securing information beyond 2010 (and 3072-bit keys for securing information beyond 2030).

Since XML Signature 1.0 required implementations to support DSA-based digital signatures, this XML Signature 1.1 revision REQUIRES signature verifiers to implement DSA in order to guarantee interoperability with XML Signature 1.0 generators. XML Signature 1.1 implementations MAY but are NOT REQUIRED to support DSA-based signature generation. We do not recommend use of DSA with 1024-bit prime moduli for signatures that will be verified beyond 2010. Longer available values as defined in SP800-57 should be used.

Since XML Signature 1.0 requires implementations to support DSA-based digital signatures, this XML Signature 1.1 revision REQUIRES signature verifiers to implement DSA only for keys of 1024 bits in order to guarantee interoperability with XML Signature 1.0 generators. XML Signature 1.1 implementations MAY but are NOT REQUIRED to support DSA-based signature generation, and given the short key size and the SP800-57 guidelines, DSA with 1024-bit prime moduli SHOULD NOT be used for signatures that will be verified beyond 2010.

Cynthia Martin 6/23/09 3:53 PM
Deleted: q value

Cynthia Martin 6/23/09 3:53 PM
Deleted: /256

Cynthia Martin 6/23/09 3:59 PM
Comment: I don't see this in SP 800-57. The text in 4.2.4.1 DSA talks about 1028, 2048 and 3072. Table 4 Recommended algorithms and minimum key sizes, page 66, says ECDSA Min.: f=160 and references the following: Column 3 indicates the minimum size of the parameters associated with FFC, such as DSA as defined in [FIPS186-3].

Cynthia Martin 6/23/09 4:00 PM
Deleted: required