## NAME

d2i_DSAPublicKey, i2d_DSAPublicKey, d2i_DSAPrivateKey, i2d_DSAPrivateKey, d2i_DSA_PUBKEY, i2d_DSA_PUBKEY, d2i_DSAparams, i2d_DSAparams, d2i_DSA_SIG, i2d_DSA_SIG - DSA key encoding and parsing functions.

## SYNOPSIS

```
#include <openssl/dsa.h>
#include <openssl/x509.h>

DSA * d2i_DSAPublicKey(DSA **a, const unsigned char **pp, long length);

int i2d_DSAPublicKey(const DSA *a, unsigned char **pp);

DSA * d2i_DSA_PUBKEY(DSA **a, const unsigned char **pp, long length);

int i2d_DSA_PUBKEY(const DSA *a, unsigned char **pp);

DSA * d2i_DSAPrivateKey(DSA **a, const unsigned char **pp, long length);

int i2d_DSAPrivateKey(const DSA *a, unsigned char **pp);

DSA * d2i_DSAparams(DSA **a, const unsigned char **pp, long length);

int i2d_DSAparams(const DSA *a, unsigned char **pp);

DSA * d2i_DSA_SIG(DSA_SIG **a, const unsigned char **pp, long length);

int i2d_DSA_SIG(const DSA_SIG *a, unsigned char **pp);
```

## DESCRIPTION

*d2i_DSAPublicKey()* and *i2d_DSAPublicKey()* decode and encode the DSA public key components structure.

*d2i_DSA_PUBKEY()* and *i2d_DSA_PUBKEY()* decode and encode an DSA public key using a SubjectPublicKeyInfo (certificate public key) structure.

*d2i_DSAPrivateKey()*, *i2d_DSAPrivateKey()* decode and encode the DSA private key components.

*d2i_DSAparams()*, *i2d_DSAparams()* decode and encode the DSA parameters using a **Dss-Parms** structure as defined in RFC2459.

*d2i_DSA_SIG()*, *i2d_DSA_SIG()* decode and encode a DSA signature using a **Dss-Sig-Value** structure as defined in RFC2459.

The usage of all of these functions is similar to the *d2i_X509()* and *i2d_X509()* described in the *d2i_X509(3)* manual page.

## NOTES

The **DSA** structure passed to the private key encoding functions should have all the private key components present.

The data encoded by the private key functions is unencrypted and therefore offers no private key security.

The **DSA_PUBKEY** functions should be used in preference to the **DSAPublicKey** functions when encoding public keys because they use a standard format.

The **DSAPublicKey** functions use an non standard format the actual data encoded depends on the value of the **write_params** field of the **a** key parameter. If **write_params** is zero then only the **pub_key** field is encoded as an **INTEGER**. If **write_params** is 1 then a **SEQUENCE**

consisting of the **p**, **q**, **g** and **pub_key** respectively fields are encoded.

The **DSAPrivateKey** functions also use a non standard structure consiting consisting of a SEQUENCE containing the **p**, **q**, **g** and **pub_key** and **priv_key** fields respectively.

## SEE ALSO

*d2i_X509(3)*

## HISTORY

TBA