NAME

    X509V3_set_ctx, X509V3_set_issuer_pkey - X.509 v3 extension generation utilities

SYNOPSIS

    #include <openssl/x509v3.h>

    void X509V3_set_ctx(X509V3_CTX *ctx, X509 *issuer, X509 *subject,
            X509_REQ *req, X509_CRL *crl, int flags);
    int X509V3_set_issuer_pkey(X509V3_CTX *ctx, EVP_PKEY *pkey);

DESCRIPTION

    X509V3_set_ctx() fills in the basic fields of *ctx* of type **X509V3_CTX**, providing details potentially needed by functions producing X509 v3 extensions, e.g., to look up values for filling in authority key identifiers. Any of *subject*, *req*, or *crl* may be provided, pointing to a certificate, certification request, or certificate revocation list, respectively. When constructing the subject key identifier of a certificate by computing a hash value of its public key, the public key is taken from *subject* or *req*. Similarly, when constructing subject alternative names from any email addresses contained in a subject DN, the subject DN is taken from *subject* or *req*. If *subject* or *crl* is provided, *issuer* should point to its issuer, for instance to help generating an authority key identifier extension. Note that if *subject* is provided, *issuer* may be the same as *subject*, which means that *subject* is self-issued (or even self-signed). *flags* may be 0 or contain **X509V3_CTX_TEST**, which means that just the syntax of extension definitions is to be checked without actually producing an extension, or **X509V3_CTX_REPLACE**, which means that each X.509v3 extension added as defined in some configuration section shall replace any already existing extension with the same OID.

    X509V3_set_issuer_pkey() explicitly sets the issuer private key of the certificate that has been provided in *ctx*. This should be done for self-issued certificates (which may be self-signed or not) to provide fallback data for the authority key identifier extension.

RETURN VALUES

    X509V3_set_ctx() and **X509V3_set_issuer_pkey()** return 1 on success and 0 on error.

SEE ALSO

    X509_add_ext(3)

HISTORY

    X509V3_set_issuer_pkey() was added in OpenSSL 3.0.

    CTX_TEST was deprecated in OpenSSL 3.0; use X509V3_CTX_TEST instead.

COPYRIGHT

Copyright 2015-2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.