## NAME

**es256_pk_new**, **es256_pk_free**, **es256_pk_from_EC_KEY**, **es256_pk_from_EVP_PKEY**, **es256_pk_from_ptr**, **es256_pk_to_EVP_PKEY** - FIDO2 COSE ES256 API

## SYNOPSIS

**#include <openssl/ec.h>**
**#include <fido/es256.h>**

*es256_pk_t **
**es256_pk_new**(*void*);

*void*
**es256_pk_free**(*es256_pk_t **pkp*);

*int*
**es256_pk_from_EC_KEY**(*es256_pk_t *pk*, *const EC_KEY *ec*);

*int*
**es256_pk_from_EVP_PKEY**(*es256_pk_t *pk*, *const EVP_PKEY *pkey*);

*int*
**es256_pk_from_ptr**(*es256_pk_t *pk*, *const void *ptr*, *size_t len*);

*EVP_PKEY **
**es256_pk_to_EVP_PKEY**(*const es256_pk_t *pk*);

## DESCRIPTION

ES256 is the name given in the CBOR Object Signing and Encryption (COSE) RFC to ECDSA over P-256 with SHA-256. The COSE ES256 API of *libfido2* is an auxiliary API with routines to convert between the different ECDSA public key types used in *libfido2* and *OpenSSL*.

In *libfido2*, ES256 public keys are abstracted by the *es256_pk_t* type.

The **es256_pk_new**() function returns a pointer to a newly allocated, empty *es256_pk_t* type. If memory cannot be allocated, NULL is returned.

The **es256_pk_free**() function releases the memory backing **pkp*, where **pkp* must have been previously allocated by **es256_pk_new**(). On return, **pkp* is set to NULL. Either *pkp* or **pkp* may be NULL, in which case **es256_pk_free**() is a NOP.

The **es256_pk_from_EC_KEY**() function fills *pk* with the contents of *ec*. No references to *ec* are kept.

The **es256_pk_from_EVP_PKEY**() function fills *pk* with the contents of *pkey*. No references to *pkey* are kept.

The **es256_pk_from_ptr**() function fills *pk* with the contents of *ptr*, where *ptr* points to *len* bytes. The *ptr* pointer may point to an uncompressed point, or to the concatenation of the x and y coordinates. No references to *ptr* are kept.

The **es256_pk_to_EVP_PKEY**() function converts *pk* to a newly allocated *EVP_PKEY* type with a reference count of 1. No internal references to the returned pointer are kept. If an error occurs, **es256_pk_to_EVP_PKEY**() returns NULL.

## RETURN VALUES

The **es256_pk_from_EC_KEY**(), **es256_pk_from_EVP_PKEY**(), and **es256_pk_from_ptr**() functions return FIDO_OK on success. On error, a different error code defined in <*fido/err.h*> is returned.

## SEE ALSO

eddsa_pk_new(3), es384_pk_new(3), fido_assert_verify(3), fido_cred_pubkey_ptr(3), rs256_pk_new(3)