NAME

fido_cred_verify, **fido_cred_verify_self** - verify the attestation signature of a FIDO2 credential

SYNOPSIS

#include <fido.h>

int
fido_cred_verify(*const fido_cred_t *cred*);

int
fido_cred_verify_self(*const fido_cred_t *cred*);

DESCRIPTION

The **fido_cred_verify**() and **fido_cred_verify_self**() functions verify whether the attestation signature contained in *cred* matches the attributes of the credential. Before using **fido_cred_verify**() or **fido_cred_verify_self**() in a sensitive context, the reader is strongly encouraged to make herself familiar with the FIDO2 credential attestation process as defined in the Web Authentication (webauthn) standard.

The **fido_cred_verify**() function verifies whether the client data hash, relying party ID, credential ID, type, protection policy, minimum PIN length, and resident/discoverable key and user verification attributes of *cred* have been attested by the holder of the private counterpart of the public key contained in the credential's x509 certificate.

Please note that the x509 certificate itself is not verified.

The attestation statement formats supported by **fido_cred_verify**() are *packed*, *fido-u2f*, and *tpm*. The attestation type implemented by **fido_cred_verify**() is *Basic Attestation*.

The **fido_cred_verify_self**() function verifies whether the client data hash, relying party ID, credential ID, type, protection policy, minimum PIN length, and resident/discoverable key and user verification attributes of *cred* have been attested by the holder of the credential's private key.

The attestation statement formats supported by **fido_cred_verify_self**() are *packed* and *fido-u2f*. The attestation type implemented by **fido_cred_verify_self**() is *Self Attestation*.

Other attestation formats and types are not supported.

RETURN VALUES

The error codes returned by **fido_cred_verify**() and **fido_cred_verify_self**() are defined in <*fido/err.h*>. If *cred* passes verification, then FIDO_OK is returned.

SEE ALSO

fido_cred_new(3), fido_cred_set_authdata(3)