NAME

Net::DNS::SEC::EdDSA – DNSSEC EdDSA digital signature algorithm

SYNOPSIS

```
require Net::DNS::SEC::EdDSA;

$signature = Net::DNS::SEC::EdDSA->sign( $sigdata, $private );

$validated = Net::DNS::SEC::EdDSA->verify( $sigdata, $keyrr, $sigbin );
```

DESCRIPTION

Implementation of EdDSA Edwards curve digital signature generation and verification procedures.

sign

```
$signature = Net::DNS::SEC::EdDSA->sign( $sigdata, $private );
```

Generates the wire-format signature from the sigdata octet string and the appropriate private key object.

verify

```
$validated = Net::DNS::SEC::EdDSA->verify( $sigdata, $keyrr, $signature );
```

Verifies the signature over the sigdata octet string using the specified public key resource record.

ACKNOWLEDGMENT

Thanks are due to Eric Young and the many developers and contributors to the OpenSSL cryptographic library.

COPYRIGHT

LICENSE

SEE ALSO

Net::DNS, Net::DNS::SEC, RFC8032, RFC8080, OpenSSL <http://www.openssl.org/docs>