NAME

Net::DNS::SEC::ECCGOST − DNSSEC ECC−GOST digital signature algorithm

SYNOPSIS

```
    require Net::DNS::SEC::ECCGOST;

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

DESCRIPTION

Implementation of GOST R 34.10−2001 elliptic curve digital signature verification procedure.

sign

Signature generation is not implemented.

verify

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

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

COPYRIGHT

Copyright (c)2014,2018 Dick Franks.

All rights reserved.

LICENSE

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of the author not be used in advertising or publicity pertaining to distribution of the software without specific prior written permission.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SEE ALSO

Net::DNS, Net::DNS::SEC, Digest::GOST, RFC4357, RFC4490, RFC5832, RFC5933, RFC7091