

NAME

Net::DNS::SEC – DNSSEC extensions to Net::DNS

SYNOPSIS

```
use Net::DNS;
```

The Net::DNS::SEC module implements a few class methods used by the other modules in this suite and a few functions that can be exported.

DESCRIPTION

The Net::DNS::SEC suite provides the resource records that are needed for DNSSEC (RFC 4033, 4034 and 4035). In addition the DLV RR, a clone of the DS RR is supported (RFC 4431)

It also provides support for SIG0. That later is useful for dynamic updates using key-pairs.

RSA and DSA crypto routines are supported.

For details see Net::DNS::RR::RRSIG, Net::DNS::RR::DNSKEY, Net::DNS::RR::NSEC, Net::DNS::RR::DS, Net::DNS::RR::DLV, and see Net::DNS::RR::SIG and Net::DNS::RR::KEY for the use with SIG0.

Net::DNS contains all needed hooks to load the Net::DNS::SEC extensions when they are available.

See Net::DNS for general help.

Utility function

Use the following construct if you want to use thos function in your code.

```
use Net::DNS::SEC qw( key_difference );
```

key_difference

```
$result=key_differnece(\@a,\@b,\@result);
```

Fills @result with all keys in the array “@a” that are not in the array “@b”.

Returns 0 on success or an error message on failure.

Class methods

These functions are inherited by relevant Net::DNS::RR classes. They are not exported.

algorithm

```
$value=Net::DNS::SEC->algorithm( "RSASHA1" );
$value=$self->algorithm( "RSASHA1" );
$value=$self->algorithm(5);
```

```
$algorithm=$self->algorithm();
$mnemonic=$self->algorithm( "mnemonic" );
```

The algorithm method is used to set or read the value of the algorithm field in Net::DNS::RR::DNSKEY and Net::DNS::RR::RRSIG.

If supplied with an argument it will set the algorithm accordingly, except when the argument equals the string “mnemonic” the method will return the mnemonic of the algorithm.

Can also be called as a class method to do Mnemonic to Value conversion.

digtype

```
$value=$self->digtype( "SHA1" );
$value=$self->digtype(1);

$algorithm=$self->digtype();
$mnemonic=$self->digtype( "mnemonic" );
```

The algorithm method is used to set or read the value of the digest or hash algorithm field in Net::DNS::RR::DS and Net::DNS::RR::NSEC3 objects.

If supplied with an argument it will set the digetstype/hash algorithm accordingly, except when the argument equals the string “mnemonic” the method will return the mnemonic of the digetstype/hash algorithm.

Can also be called as a class method to do Mnemonic to Value conversion, note however that it will then use the “Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms” and not the



“DNSSEC NSEC3 Hash Algorithms” IANA registry. If you want to specifically get access to the NSEC3 digest types then use a construct like:

```
    bless $self, Net::DNS::RR::NSEC3;  
    $self->digtype( "SHA1" );
```

COPYRIGHT

Copyright (c) 2001–2005 RIPE NCC. Author Olaf M. Kolkman <olaf@net-dns.org>

All Rights Reserved

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, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS; IN NO EVENT SHALL AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

SEE ALSO

<http://www.net-dns.org/> <<http://www.net-dns.org/>>

perl(1), Net::DNS, Net::DNS::RR::KEY, Net::DNS::RR::SIG, Net::DNS::RR::DNSKEY, Net::DNS::RR::RRSIG, Net::DNS::RR::NSEC, Net::DNS::RR::DS, Net::DNS::SEC::Private.

RFC4033, 4034 and 4035.

