

Re: Using Crypt::DSA

Source: <http://coding.derkeiler.com/Archive/Perl/comp.lang.perl.misc/2005-08/msg01711.html>

- *From:* "Sisyphus" <sisyphus1@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 27 Aug 2005 09:04:05 +1000
-

"Mike Friedman" <mikef@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

[snip]

- >
- > I want to be able to create a public key file and a signature in formats
- > that can be distributed to a user community whose applications may be
- > using other DSA implementations (e.g., Java crypto lib, or other scripting
- > languages besides perl). So, it's important that the public key file be
- > in a reasonably standard format.

Which, afaik, would be a pem file. Crypt::DSA can parse them (as long as you have Convert::PEM) and so, presumably, can the other DSA implementations. To write a *public* key pem file with Crypt::DSA you just do (as in 04-pem.t):

```
$key->priv_key(undef);  
$key->write( Type => 'PEM', Filename => $keyfile);
```

- > Also, I'd be passing the signature as
- > a base64-encoded string via a web form field. Once the application
- > base64-decodes it, the signature should be in a format easily fed to its
- > DSA verify routine.
- >

Are you saying the signature part is not a problem ? I find some ambiguity with "the signature should be in a format easily fed to its DSA verify routine" – not sure whether that means the signature is already in a suitable format, or whether it means that it needs to be in a suitable format (but isn't).

Cheers,
Rob

.

- *Follow-Ups:*
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* Mike Friedman

- *References:*
 - ◆ [Using Crypt::DSA](#)
 - ◇ *From:* Mike Friedman
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* A. Sinan Unur
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* Mike Friedman
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* Sisyphus
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* Mike Friedman
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* Sisyphus
 - ◆ [Re: Using Crypt::DSA](#)
 - ◇ *From:* Mike Friedman

- Prev by Date: [Re: object "loses values" when other object created](#)
- Next by Date: [Re: Perl regular expressions help](#)
- Previous by thread: [Re: Using Crypt::DSA](#)
- Next by thread: [Re: Using Crypt::DSA](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)