

Re: Gnupg

Source: <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2006-01/msg03577.html>

- *From:* Phillip Susi <psusi@xxxxxxxxxx>
 - *Date:* Tue, 31 Jan 2006 10:21:27 -0500
-

Old Rucker wrote:

Maybe a bit OT, but S/MIME (which I wouldn't call standard....) is much

It's just as standard as ordinary RFC 822 mime encoded email.

less secure than the algorithms used in GPG and can be broken relatively easily. However, for most purposes its adequate providing you haven't got sensitive stuff being encrypted.

This is completely untrue; it uses the the strongest algorithms available. Specifically either MD5 or SHA1 are usually used for fingerprinting and RSA or DSA (typically 1024 bit) are used for public/private key signing/encryption, with typically a 128 bit 3DES or AES cipher used to encrypt the message body, using a random key which is then encrypted using each recipient's public key.

Baring a compromise of your private key (meaning both the certificate file as well as the password used to encrypt it), the system is unbreakable.

Probably an exaggeration, but don't forget the US Secret Service once said that if all the personal computers in the world were set to crack one PGP encrypted message, it would taken ten times the age of the universe to crack it. The algorithms used in later versions of PGP and now GPG are much more secure, and I'd rather use just one system for my encryption and signing that works.

I'd rather use just one as well, and I prefer to use the one that is an based on ISO standards (x.509, PKCS, etc) rather than a home brewed

Re: Gnupg

"one off" open source solution.

However, the OP was asking about GPGME, which is a library that allows the integration of GPG into a package that doesn't yet support it.

Use libopenssl instead ;)

--

ubuntu-users mailing list

ubuntu-users@xxxxxxxxxxxxxxxxxxxx

<https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>