A NOTE OF WARNING

My public key lets you do either or both of two things:

(a) encrypt a message so that only the use of the corresponding private key will make it intelligible; or

(b) verify that a signature attached to a message was made by the corresponding private key.

What good does that do, in either case?

It depends how good I am at ensuring that the private key remains under my sole control. If I am the only person who can use the key to decrypt documents, then I am the only person who can understand messages encrypted with the public key. And if I am the only person who can use the key to sign a message, a signature verified by the public key must have been made by me.

But of course there is a snag, because neither of those conditions can be reliably assured. Both are based on (fairly) modern cryptography, and that depends on the use of computers to carry out the necessary cryptographic functions. Computers, especially when connected to the Internet, are not secure. They are vulnerable to attacks using malicious software and other techniques. These sometimes exploit software errors, such as errors in the implementation of cryptographic functions or procedures. I take what I think are reasonable precautions to protect my private key, but I cannot be sure that they are sufficient; and I stand no chance of detecting software errors. So I can give no guarantees. And if it turns out that my precautions are insufficient, then unknown third parties may be able to read encrypted documents meant for my eyes only, and may be able to attach signatures to messages which will verify correctly using my public key.

Using my public key is better than not using it; but neither you nor I can really know how much better. Proceed with caution; and don't blame me if it goes wrong.

So I offer my public key on the following terms:

1 My public key is for your personal use only. Make as many copies as you need, but do not provide it to anyone else. Instead, direct them to this web page.

2 If I sign something with my private key, I accept the signature as binding. But if I repudiate a signature, even if my public key verifies it, then it is for you to show that I made or authorised the signature (just as for any other kind of signature that I reject as a forgery).

3 Downloading my public key is acceptance of these terms.

Accept the terms and get my public key Go back to previous page