

My keys

Secure communication across the internet requires cryptography.

This page documents the keys I use.

For email I use PGP/GPG - I have never seen the point of S/MIME - and I don't use the Danish Digital Signature.

For remote logon across the internet I use ssh protocol version 2 (I refuse to use telnet/rlogin).

Before using these keys be sure to verify them by some other means than this page (call me, email me or check the signatures on my pgp key and if you find someone you know, then use gpg/pgp to verify the signatures of my ssh keys).

PGP/GPG for e-mail

My public key is keyid 0xD1EFBAA6 and is connected to my primary e-mail addresses hlk@kramse.dk and hlk@security6.net:

```
$ gpg --fingerprint hlk@kramse.dk
pub 1024D/D1EFBAA6 2003-01-20
Key fingerprint = 0FAE F19D DB46 DF2E D93D 9B05 21A6 469B D1EF BAA6
uid Henrik Lund Kramshoej (work email) <hik@security6.net>
uid Henrik Lund Kramshoej (Kramse) <hik@kramse.dk>
sub 2048g/6D08E6E6 2003-01-20
```

It can be downloaded [here](#) or found using the MIT PGP Keyserver or other places: <http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xD1EFBAA6>

Verifying keys

Files downloaded from the internet cannot be trusted - so you need to verify my key after downloading it. The best verification is when you and I meet face to face and I tell you my fingerprint - which you can verify when you have found a key that seems to be mine. I have my fingerprint on my business card so having a physical piece of paper from me can be used to verify the authenticity of the key you downloaded from here or any keyserver.

It might be impractical for us to meet, for instance if you are in a place far from Denmark. Second best verification is if you have verified the key of somebody you trust and she and I have meet at some point in time and signed PGP keys. This verification is called web of trust and the only thing that is being verified is that the keys used belong to the people in between.

For instance I was at the SANE conference in Holland and there was a keymaster called Teujn Nissen who signed my key. I know from his behaviour that he checked my passport and so his signature on my key is proof that my key belongs to me.

Default Publication

Whenever I find a key signed by this person I can trust that he did some identity checking and so I can trust the key of Wietse Venema who is the author of Postfix.

By signing other peoples keys you help extend the web of trust and make it easier to verify that keys do in fact belong to the persons involved.

To help you verify the paths from you to me through this web of trust you can use a PGP pathfinder. The PGP pathfinder then tries to find trust paths between arbitrary keys.

You can use it to find paths between your key and mine:

http://www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/mk_path.cgi

Secure Shell

Sometimes I need access to a computer set up by others and they can send me the password using encrypted e-mail - see GPG above - or use my SSH public key.

The key I use can be downloaded [here](#) and verified with this [signature](#) (if you have verified my PGP key first of course).

Installing my SSH key

First you should add a user - I prefer user id hlk then make the directory .ssh and install the key with the correct ownership and permissions.

```
# cd ~hlk
# mkdir .ssh
# cat kramse-public-ssh.txt > .ssh/authorized_keys
# chown -R hlk .ssh
# chmod -R go-rwx .ssh
```