with the macro `DKKEY_DIR`. Be sure this directory is readable by `exim` but not by
the rest of the world.

```
### macros to define the directories for databases and keys
CONFIG_DIR = path_to_config_dir
DKKEY_DIR = path_to_key_dir

### main section: define the domains to sign and required DKIM acl
domainlist dksign_domains = cdb;CONFIG_DIR/dk.selector.cdb
acl_smtp_dkim = acl_process_dkim

### ACL section: verify signature on incoming mail, add a header
acl_process_dkim:
  warn !dkim_status = none
  add_header = :at_start:X-DKIM-Report: $dkim_verify_status \n  $(!eq{$dkim_verify_status}{pass}{$dkim_verify_reason }{} \n  {Signer=$dkim_cur_signer} {Testing=$dkim_key_testing}

### Router section: put just before "dnslookup" router, sign nonlocal
dnslookup_signed:
  driver = dnslookup
domains = !+local_domains
transport = remote_dksign
condition = ${if match_domain{$sender_address_domain} \n  {+dksignDomains}}
no_verify

### Transport section: does the actual signing
remote_dksign:
  driver = smtp
dkim_domain = $sender_address_domain
dkim_selector = ${lookup {dkim_domain} \ncdb{CONFIG_DIR/dk.selector.cdb} {value}fail}
dkim_private_key = DKKEY_DIR/rsa.private.$dkim_selector.$dkim_domain
dkim_strict = 1
```

These fragments result in outgoing messages being signed and incoming mes-
sages having their signatures verified and a DKIM report header added. Here's an
example of that header:

```
X-DKIM-Report: pass (Signer=gmail.com) (Testing=0)
```

Further policy is needed if you are going to reject or punish messages whose sig-
natures do not verify.

The `no_verify` line in the router section refers not to DKIM verification but rather
to verifying the recipient's address; it is turned off in this router, but done in the
dnslookup router that is next in line. No sense doing it twice.

**DKIM in Postfix**

DKIM is implemented in Postfix with the DKIM-milter software package de-
scribed on page 846. Generate your key pair and test it with `dkim-testkey`; build a