

## Random Number Generation

The PCI-PTS approved random generator shall be used when random numbers are required by the SRED encryption scheme and have to be generated by the application code.

Use the character special file `"/dev/urandom"` or `"/dev/random"` for getting the values from the approved random number generator; e.g.

### Example: get random number

```
int get_random(void *buf, size_t len) {    int rc;    int fd = open(
"/dev/urandom", O_RDONLY);    if (fd < 0) {        rc = fd;    }
else {        rc = read(fd, buf, len);        close(fd);    }    return
rc;}
```