

**NAME**

`pki --pub` - Extract a public key from a private key or certificate

**SYNOPSIS**

**pki --pub**[**--in** *file*][**--keyid** *hex*] [**--type** *type*] [**--outform** *encoding*] [**--debug** *level*]

**pki --pub--options** *file*

**pki --pub-h** | **--help**

**DESCRIPTION**

This sub-command of **pki**(1) extracts public keys from a private keys and certificates.

**OPTIONS**

**-h, --help**

Print usage information with a summary of the available options.

**-v, --debug** *level*

Set debug level, default: 1.

**-+, --options** *file*

Read command line options from *file*.

**-i, --in** *file*

Input file. If not given the input is read from *STDIN*.

**-x, --keyid** *hex*

Smartcard or TPM private key object handle in hex format with an optional 0x prefix.

**-t, --type** *type*

Type of input. One of *priv* (private key), *rsa* (RSA private key), *ecdsa* (ECDSA private key), *pub* (public key), *pkcs10* (PKCS#10 certificate request), or *x509* (X.509 certificate), defaults to *priv*.

**-f, --outform** *encoding*

Encoding of the extracted public key. One of *der* (ASN.1 DER), *pem* (Base64 PEM), *dnskey* (RFC 3110 DNS key), or *sshkey* (RFC 4253 SSH key), defaults to *der*.

**EXAMPLES**

Extract the public key from an RSA private key:

```
pki --pub --in key.der > pub.der
```

Extract the public key from an X.509 certificate:

```
pki --pub --in cert.der --type x509 > pub.der
```

**SEE ALSO**

**pki(1)**