Signing Files

Banded Authentication Distribution Incorporated

October 2015

1 Signing and Verifying Files:

This document serves as a information document that demonstates how to sign and verify software packages via the use of openssl and rsa keys.

1.1 Key Pair

To generate a rsa key pair, use the following commands:

To generate the rsa private key:

```
$ openssl genrsa -out [privatekey] 4096
```

To generate the rsa public key:

```
$ openssl rsa -pubout -in [privatekey] -out [publickey]
```

2 Signing:

To create a signature of a binary file:

```
$ openssl dgst -sha1 -sign [privatekey] [file] > [signature]
```

3 Verifying:

To verify a signature of a binary file:

```
$ openssl dgst -sha1 -verify [publickey] -signature [signature] [file]
```